CAN THE USE OF FACTUAL DATA ANALYSIS STRENGTHEN NATIONAL SECURITY? PART TWO

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

MAY 20, 2003

Serial No. 108–98

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

91–646 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
JOHN SULLIVAN, Oklahoma
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
WILLIAM J. JANKLOW, South Dakota
MARSHA BLACKBURN, Tennessee

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. "DUTCH" RUPPERSBERGER, Maryland
ELEANOR HOLMES NORTON, District of Columbia
JIM COOPER, Tennessee
CHRIS BELL, Texas

BERNARD SANDERS, Vermont (Independent)

PETER SIRH, *Staff Director*
MELISSA WOJCIAK, *Deputy Staff Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHILIP M. SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

ADAM H. PUTNAM, Florida, *Chairman*

CANDICE S. MILLER, Michigan
DOUG OSE, California
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio

WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

EX OFFICIO

TOM DAVIS, Virginia

HENRY A. WAXMAN, California

BOB DIX, *Staff Director*
SCOTT KLEIN, *Professional Staff Member*
URSULA WOJCIECHOWSKI, *Clerk*
DAVID MCMILLEN, *Minority Professional Staff Member*

CONTENTS

CAN THE USE OF FACTUAL DATA ANALYSIS STRENGTHEN NATIONAL SECURITY? PART TWO

TUESDAY, MAY 20, 2003

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:04 a.m., in room 2154, Rayburn House Office Building, Hon. Adam H. Putnam (chairman of the subcommittee) presiding.

Present: Representatives Putnam, Miller, Turner, Clay and Lynch.

Staff present: Bob Dix, staff director; John Hambel, senior counsel; Scott Klein, Chip Walker, Lori Martin, and Casey Welch, professional staff members; Ursula Wojciechowski, clerk; Suzanne Lightman, fellow; Bill Vigen, intern; David McMillen, minority professional staff member; and Jean Gosa, minority assistant clerk.

Mr. PUTNAM. A quorum being present, this hearing of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order.

Good morning and welcome to today's hearing entitled, "Can the Use of Factual Data Analysis Strengthen National Security, Part Two."

With today's continued improvements in technology, particularly in the areas of data base exploration and information sharing, Federal agencies faced with the monumental task of enhancing national security and law enforcement are provided a number of opportunities to do so more effectively. Specifically, the process of factual data analysis enables the end user to sort through massive amounts of information, identifying patterns of interest to its user in a matter of seconds. This type of tool has proven beneficial in a variety of applications and could have considerable implications for law enforcement and Federal authorities tasked with identifying terrorist activity before it strikes.

At the same time, there are valid questions and concerns about the Government's potential access to the personal information of individual citizens that could be the subject of a data mining process. While it is important that the Federal Government utilize all available resources to enhance national security, it is critical that we continue to safeguard American values of personal freedom and privacy.

Today's hearing will focus on examining the questions and concerns surrounding the Federal Government's use of factual data analysis or information produced by this analytical process. With the wealth of technology available today and certainly as a result of the events of September 11, 2001, the American people have a realistic expectation that government and law enforcement entities must continue their efforts to become better equipped to perform their duties.

Many Federal agencies do not even have the technological tools that the private sector currently possesses. In many cases, this means that agencies are undergoing a complete technology upgrade as well as introducing advanced information technology applications. Advanced technology will enable Government to better share and analyze important information. By making use of these tools, Government and law enforcement hope to be more successful at securing and protecting our Nation.

As Government and law enforcement begin to implement new strategies using advanced technology such as data mining, there are a number of questions and concerns that need to be addressed. These agencies will need to address how existing privacy laws would apply to their programs, what data sources do they intend to draw from, how the reliability of the data will be ensured, what procedures are in place to secure the data collected from intrusion, and what recourse would be available to an individual who believes his or her information is inaccurate or incomplete.

We have held previous hearings on this topic. On May 6, the subcommittee heard from representatives from the Total Information Awareness Program run by the Defense Advanced Research Project Agencies, the Transportation Security Administration's CAPPII Program which is a passenger pre-screening process, the FBI's Trilogy, related data warehousing and data mining programs.

What we learned from each of these witnesses is that they are in the very infant stages of developing their strategies involving this analytical process. They have testified that as they continue to figure out what role factual data analysis will play, each acknowledge and affirm their commitment to protection of privacy and personal freedom as fundamental elements of their program.

Today, we will hear from an expert panel of witnesses who will address the matter of privacy, confidentiality and personal freedom in the context of the protection of civil liberties in the pursuit of homeland security and strengthen law enforcement. The members of the subcommittee look forward to hearing the observations and recommendations from this panel and to continue to examine these matters to determine if in fact factual data analysis can strengthen national security.

The use of advanced information technologies does not mean the erosion of personal liberties is inevitable. The Federal Government's objective of better information sharing and analysis can and must be met simultaneously with that of securing personal liberties. The subcommittee looks forward to working with these agencies and the variety of stakeholders in this matter in implementing their planned proposals for enhancing homeland security using advanced information technology.

Today's hearing can be viewed live via Web cast by going to reform.house.gov and clicking on the link under live committee broadcast.

I am pleased to yield to the distinguished vice chairman of the subcommittee, the gentlelady from Michigan, Mrs. Miller, for her opening statement.

[The prepared statement of Hon. Adam H. Putnam follows:]

COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS
CONGRESSMAN ADAM PUTNAM, CHAIRMAN

OVERSIGHT HEARING
STATEMENT BY ADAM PUTNAM, CHAIRMAN

Hearing topic: *"Can Factual Data Analysis Strengthen National Security? -Part Two"*

Tuesday, May 20, 2003
10:00 a.m.
Room 2154 Rayburn House Office Building

OPENING STATEMENT

With today's continued improvements in technology, particularly in the areas of database exploration and information sharing, Federal agencies faced with the monumental task of enhancing national security and law enforcement, are provided a number of opportunities to do so more effectively. Specifically, the process of factual data analysis enables the end user to sort through massive amounts of information, identifying patterns of interest to its user, in a matter of seconds. This kind of tool has proven to be beneficial in a variety of applications, and could have considerable implications for law enforcement and Federal authorities tasked with identifying terrorist activity before it strikes.

At the same time, there are valid questions and concerns about the government's potential access to the personal information of individual citizens that could be the subject of a "data mining" process. While it is important that the Federal government utilize all available resources to enhance national security, it is critical that we continue to safeguard American values of personal freedom and privacy. Today's hearing will focus on examining the questions and concerns surrounding the federal government's use of factual data analysis, or information produced by this analytical process.

With the wealth of technology available today, and certainly as a result of the events of September 11, 2001, the American people have a realistic expectation that government and law enforcement entities must continue their efforts to become better equipped to perform their duties. Many Federal agencies do not even have the technological tools that the private sector currently posses. In many cases, this means that agencies are undergoing a complete technology upgrade as well as introducing advanced information technology applications. Advanced technology will enable government to better share and analyze important information.

By making use of these tools, government and law enforcement hope to be more successful at securing and protecting our nation.

As government and law enforcement begin to implement new strategies using advanced technologies such as data mining, there are a number of questions and concerns that need to be addressed. These agencies will need to address how existing privacy laws would apply to their programs; what data sources do they intend to draw from; how the reliability of the data will be insured; what procedures would be in place to secure the data collected from intrusion; and what recourse would be available to an individual who believes that his or her information is inaccurate or incomplete.

We have held previous hearings on this very subject. On May 6th, the Subcommittee heard from representatives from the Total Information Awareness program, which is run by Defense Advanced Research Projects Agency, the Transportation Security Administration's CAPPS II program, which is a passenger prescreening process, and the FBI's Trilogy and related data warehousing and data mining programs. What we learned from each of these witnesses is that they are in the very infancy stages of developing their strategies involving this analytical process. They have testified that as they continue to figure out what role factual data analysis will play, each acknowledge and affirm their commitment to protection of privacy and personal freedom as fundamental elements of their program.

Today we will hear from an expert panel of witnesses who will address the matter of privacy, confidentiality and personal freedom, in the context of the protection of civil liberties in the pursuit of homeland security and strengthened law enforcement. The members of the Subcommittee look forward to hearing the observations and recommendations from this panel and to continue to examine these matters to determine in fact, whether "factual data analysis" can strengthen national security.

The use of advanced information technologies does not mean the erosion of personal liberties is inevitable. The federal government's objective of better information sharing and analysis can...and must... be met simultaneously with the securing of personal liberties. The Subcommittee looks forward to working with these agencies and the variety of stakeholders in this matter, as they continue to plan and implement their proposals for enhancing homeland security using advanced information technology.

Mrs. MILLER. Thank you, Mr. Chairman.

As we begin the third subcommittee hearing on factual data analysis, the issue of privacy protection becomes exceedingly important. In previous hearings as you mentioned, we heard testimony from representatives of the Department of Defense, the Transportation Security Administration, and the FBI, all insisting that the privacy of citizens would not be compromised and certainly that those agencies are very sensitive to concern raised about the invasion of personal privacy by Big Brother or by Government.

In the written testimony submitted for today's hearing by Mr. Rosenzweig, he states, "Fundamental legal principles and conceptions of American Government should guide the configuration of our intelligence and law enforcement rather than the reverse." One of the hallowed principles certainly of our American system is that we the people determine what the government can and cannot and should not do, not the other way around.

This subcommittee has primary oversight of the technology initiatives of the Federal Government and as Federal agencies begin to integrate and streamline information technologies, it is very important that the processes associated with Federal actions remain transparent so that the confidence of the American people is not lost. We find ourselves today in a highly salient national debate concerning the balance between national security and personal privacy. Factual data analysis is a tool that will better enable local, State and Federal officials to secure the homeland from terror attacks and because of the power and the breadth of capabilities associated with this tool, both now and in the future, high scrutiny of its implementation is required.

Mr. Cohen, in his written testimony, has cited instances where the potential for abuse of factual data analysis will be ever present but potential abuse exists currently in all levels of Government activity and hopefully through the work of this subcommittee, we can help Americans view the implementation of improved data mining techniques and its homeland security benefits with cautious optimism and not with fear. I am confident that the rights of American citizens outlined by the Constitution and the Bill of Rights will not be subverted in the auspices of national security.

I want to thank all three of the witnesses for coming today. I am looking forward to working with our chairman and this committee and I look forward to your testimony today.

[The prepared statement of Hon. Candice S. Miller follows:]

Congresswoman Candice S. Miller

Opening Statement
Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census
May 20, 2003

OPENING STATEMENT

Thank you, Mr. Chairman.

As we begin the third Subcommittee hearing on factual data analysis, the issue of privacy protection becomes exceedingly important. In previous hearings, we heard testimony from representatives of the Department of Defense, the Transportation Security Administration, and the FBI insisting that the privacy of citizens will not be compromised and that those agencies are very sensitive to concerns raised about invasion of personal privacy by government.

In the written testimony submitted for this hearing by Mr. Rosenzweig, he states, "Fundamental legal principles and conceptions of American government should guide the configuration of our intelligence and law enforcement efforts rather than the reverse."

One of the hallowed principles of our American system is that we, the people, determine what the government can and should do – not the other way around.

This Subcommittee has primary oversight of the technology initiatives of the Federal government. And as federal agencies begin to integrate and streamline information technologies, it is important that the processes associated with Federal actions remain transparent so that the confidence of the American people is not lost. We find ourselves in a highly salient national debate concerning the balance between national security and personal privacy.

Factual data analysis is a tool that will better enable Local, State, and Federal officials to secure the homefront from terror attacks. Because of the power and the breadth of capabilities associated with this tool, both now and in the future, high scrutiny of its implementation is required.

Mr. Cohen, in his written testimony, has cited instances where the potential for abuse of factual data analysis will be ever-present. But potential abuse exists currently at all levels of government activity. Hopefully through the work of this Subcommittee, we can help Americans view the implementation of improved data mining techniques and its homeland security benefits with cautious optimism and not with fear.

I am confident that the rights of American citizens outlined by the Constitution and the Bill of Rights will not be subverted in the auspices of national security.

I want to thank Mr. Rozenweig, Mr. Steinhardt, and Mr. Cohen for testifying today. I look forward to working with each of you as this Subcommittee oversees the implementation of factual data analysis by various Federal agencies.

Thank you, Mr. Chairman.

Mr. PUTNAM. We thank the gentlelady from Michigan and appreciate her very active involvement in the work of this subcommittee. The wealth of experience she brings from the Michigan Department of State has proven very valuable to this subcommittee. We appreciate your continued involvement.

As is the custom with the committee and its subcommittees, we will swear in our witnesses.

[Witnesses sworn.]

Mr. PUTNAM. As you are all aware, we have the lighting system. You have submitted your written statements for the record and we ask that you summarize your oral statement in 5 minutes at which time you will see the yellow light indicating the need to wrap up and the red light indicating that time has expired.

I will introduce the first of our three witnesses, Mr. Paul Rosenzweig, senior legal research fellow, the Heritage Foundation, Center for Legal and Judicial Studies. Before coming to Heritage, he was in private practice specializing in Federal, appellate and criminal law and legal ethics. Previously he served as senior litigation counsel and associate independent counsel, Office of the Independent Counsel. Before working at OIC, he worked as the chief investigative counsel for the House Committee on Transportation and Infrastructure where his work included the 1996 Value Jet crash. He received his law degree cum laude from the University of Chicago in 1986.

Welcome. You are recognized.

STATEMENTS OF PAUL ROSENZWEIG, SENIOR LEGAL RESEARCH FELLOW, CENTER FOR LEGAL AND JUDICIAL STUDIES, THE HERITAGE FOUNDATION; BARRY STEINHARDT, DIRECTOR, TECHNOLOGY AND LIBERTY PROGRAM, AMERICAN CIVIL LIBERTIES UNION; AND JOHN COHEN, CO-FOUNDER, PRESIDENT AND CEO, PSCOM LLC, INC.

Mr. ROSENZWEIG. Thank you, Mr. Chairman.

Thank you for the invitation to come and speak with you today about a topic I consider to be the single most important domestic legal issue facing Congress and the American people.

I should begin with the routine request of my Foundation that I emphasize I am here on my own account and nothing I say is a corporate position of the Heritage Foundation or its board of trustees.

Before speaking to TIA and CAPPSII directly, I would like to talk about a subject to which both of you alluded in your opening statements, the role of Congress and the vital importance of that role.

I had the pleasurable experience of meeting a couple weeks ago with Lord Alexander Carlisle who is a Lord of the House of Lords in Great Britain. As you know, Great Britain has passed a series of laws similar to our own Patriot Act which all involve the difficult question of tradeoffs between civil liberties and national security. Pursuant to that law, one of the unique steps the English have taken is that the law requires the appointment of an independent reviewer who has the power to review all the records within the holding of the Home Secretary whenever he undertakes some exercise of the newly granted terror powers, and is empowered to re-

port on those uses of the anti-terror provisions to the Parliament. Lord Carlisle is that independent reviewer and he was here in the United States to do a bit of his own comparative analysis, examining how we in America have dealt with the balance.

We don't have such a person in our provisions of the Patriot Act and in our developing understanding of TIA and CAPPS. Congress is that position. They are the independent reviewer. The genius of the founders was the system of checks and balances and the core of that genius is the use of thoughtful, sustained, non-partisan oversight of the use of the powers we give the executive branch.

There are some who would say the potential for abuse of a new system means we should forego its development. Of course any new system can be abused, but, in my judgment, the right answer is to attempt rationally to construct the systems of oversight that will enable this Congress and Congresses that come after it to examine the conduct of the executive branch and determine whether or not it is in fact appropriate and consistent with the laws we have imposed upon it.

That is my single most significant and sustained recommendation to you as you consider TIA and CAPPSII. The real questions about things like CAPPSII are not whether it will work, because in the end we will find the answer and if it doesn't work, then a lot of this debate is moot and we may have wasted a lot of money. In the end, it will be irrelevant.

The real question is, what if it does work. What will you be doing to examine whether or not it is being used appropriately or inappropriately. To do that, Congress is going to need absolute, unfettered access to information about the operation of a system like CAPPSII. What I say about CAPPSII applies equally to TIA.

In some instances, that access may require the receipt of information in a classified or confidential manner, since I know full well the disclosure of means and methods can render them utterly useless and unreasonable, but the vital factor that you should consider is making sure as you go down the development and authorization path that you require the provision of information not just about raw data, about gross numbers, but the ability for somebody, somewhere to examine individual cases. There should be an appeals process as well outside of Congress but the ultimate and final repository of the ability to check the excessive use of governmental authority rests in this body.

I see that my time is almost up which is amazing because I feel I have barely begun but in deference to the committee's time structure, and I am sure we will have the opportunity for questions, I will stop now.

[The prepared statement of Mr. Rosenzweig follows:]

TESTIMONY OF

PAUL ROSENZWEIG

SENIOR LEGAL RESEARCH FELLOW
CENTER FOR LEGAL AND JUDICIAL STUDIES

THE HERITAGE FOUNDATION*

214 MASSACHUSETTS AVENUE, NE
WASHINGTON, DC 20002

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON TECHNOLGY, INFORMATION POLCY,
INTERGOVERNMENTAL RELATIONS, AND THE CENSUS

REGARDING

CAN THE USE OF FACTUAL DATA ANALYSIS STRENGTHEN NATIONAL SECURITY? -- PART TWO

20 MAY 2003

---

* The Heritage Foundation is a public policy, research, and educational organization operating under Section 501(c)(3). It is privately supported, and receives no funds from any government at any level, nor does it perform any government or other contract work. The Heritage Foundation is the most broadly supported think tank in the United States. During 2002, it had more than 200,000 individual, foundation, and corporate supporters representing every state in the U.S. Its 2002 contributions came from the following sources: Individuals (61%); Foundations (27%); Corporations (7%); Investment Income (1%); and Publication Sales and Other (3%). Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own and do not reflect an institutional position for The Heritage Foundation or its board of trustees.

Good morning Mr. Chairman and Members of the Subcommittee. Thank you for the opportunity to testify before you today on the challenge of maintaining the balance between security and constitutionally protected freedoms inherent in responding to the threat of terror, especially in the context of data analysis or data mining.

For the record, I am a Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation, a nonpartisan research and educational organization. I am also an Adjunct Professor of Law at George Mason University where I teach Criminal Procedure and an advanced seminar on White Collar and Corporate Crime. I am a graduate of the University of Chicago Law School and a former law clerk to Judge Anderson of the U.S. Court of Appeals for the Eleventh Circuit. For much of the past 15 years I have served as a prosecutor in the Department of Justice and elsewhere, prosecuting white-collar offenses. During the two years immediately prior to joining The Heritage Foundation, I was in private practice representing principally white-collar criminal defendants. I have been a Senior Fellow at The Heritage Foundation since April 2002.

My perspective on this matter, then, is that of a lawyer and a prosecutor with a law enforcement background, not that of technologist or an intelligence officer/analyst. I should hasten to add that much of my testimony today is based upon a series of papers I have written on various aspects of this topic and testimony I have given before other bodies in Congress, all of which are available at The Heritage Foundation website (www.heritage.org). For any who might have read this earlier work, I apologize for the familiarity that will attend this testimony. Repeating myself does have the virtue of maintaining consistency -- I can only hope that any familiarity with my earlier work on the subject does not breed contempt.

* * * * *

It is a commonplace for those called to testify before Congress to commend the Representatives or Senators before whom they appear for their wisdom in recognizing the importance of whatever topic is to be discussed – so much so that the platitude is often disregarded as mere puffery. Today, however, when I commend this Subcommittee for its attention to the topic at hand – the difficulty of both protecting individual liberty and enabling our intelligence and law enforcement organizations to combat terror – it is no puffery, but rather a heartfelt view. I have said often since September 11 that the civil liberty/national security question is *the* single most significant domestic legal issue facing America today, bar none. And, as is reflected in my testimony today, in my judgment one of the most important components of a responsible governmental policy addressing this difficult question will be the sustained, thoughtful, non-partisan attention of America's elected leaders in Congress. Nothing is more likely, in my judgment, to allow America to find the appropriate balance than your engagement in this issue.

What I would like to do today is assist your consideration of this question by addressing some theoretical principles that you might consider in structuring your thinking about the problem. I would then like to briefly discuss the nature of the problem posed by terrorist threats – all too often in weighing security and liberty in the balance we focus only

on the liberty side of the ledger without really reminding ourselves of what the true nature of the threat is. Then, in an effort to avoid being too theoretical, I'd like to apply the principles I have offered to the concrete issue of data mining and analysis as it might be used in the Total Information Awareness program (TIA) and the Computer Assisted Passenger Prescreening System (CAPPS II).

But let me first give you a short, pithy answer to the question posed by the title of today's hearing: Can the use of factual data analysis strengthen national security? The answer is "Of course." The more difficult question – the one that is the focus of my testimony – is the challenging one of implementation. How can we use factual data analysis in ways that are effective and useful yet do not unnecessarily or unreasonably trench on fundamental American conceptions of civil liberty and privacy?

OVERARCHING PRINCIPLES

Let begin with some general thoughts about how cautious, yet effective governmental action can, in my view, be implemented. Fundamental legal principles and conceptions of American government should guide the configuration of our intelligence and law enforcement efforts rather than the reverse. The precise contours of any rules relating to the use of any new technology or new program will depend, ultimately, on exactly what the new program is capable of or intended to accomplish — the more powerful the system or program, the greater the safeguards necessary. As a consequence, the concerns of civil libertarian critics should be fully voiced and considered while any research program is underway.

In general, unlike civil libertarian skeptics, I believe that new intelligence and law enforcement information gathering and information analytical systems can (and should) be constructed in a manner that fosters both civil liberty and public safety. We should not say that the risks of such systems are so great that any effort to construct them should be dispensed with.

Rather in my view, the proper course is to ensure that certain overarching principles animate and control the architecture of any new program and provide guidelines that will govern implementation of the program in the domestic environment.

The Common Defense – Let me make one important preliminary point: Most of the debate over new intelligence systems focuses on perceived intrusions on civil liberties, but Americans should keep in mind that the Constitution weighs heavily on both sides of the debate over national security and civil liberties. The President and Congressional policymakers must respect and defend the individual civil liberties guaranteed in the Constitution when they act, but there is also no doubt that they cannot fail to act when we face a serious threat from a foreign enemy.

The Preamble to the Constitution acknowledges that the United States government was established in part to provide for the common defense. The war powers were granted to Congress and the President with the solemn expectation that they would be used. Congress was also granted the power to "punish ... Offenses against the Law of Nations," which include the international law of war, or terrorism. In addition, serving as chief executive and

commander in chief, the President also has the duty to "take Care that the Laws be faithfully executed," including vigorously enforcing the national security and immigration laws. Thus, as we assess questions of civil liberty I think it important that we not lose sight of the underlying end of government – personal and national security. I do not think that the balance is a zero-sum game, by any means. But it is vital that we not disregard the significant factors weighing on *both* sides of the scales.

Civil Liberty -- Of course, just because the Congress and the President have a constitutional obligation to act forcefully to safeguard Americans against attacks by foreign powers does not mean that every means by which they might attempt to act is necessarily prudent or within their power. Core American principles require that any new counter-terrorism technology deployed domestically) should be developed only within the following bounds:

- No fundamental liberty guaranteed by the Constitution can be breached or infringed upon.
- Any increased intrusion on American privacy interests must be justified through an understanding of the particular nature, significance, and severity of the threat being addressed by the program. The less significant the threat, the less justified the intrusion.
- Any new intrusion must be justified by a demonstration of its effectiveness in diminishing the threat. If the new system works poorly by, for example, creating a large number of false positives, it is suspect. Conversely, if there is a close "fit" between the technology and the threat (that is, for example, if it is accurate and useful in predicting or thwarting terror), the technology should be more willingly embraced.
- The full extent and nature of the intrusion worked by the system must be understood and appropriately limited. Not all intrusions are justified simply because they are effective. Strip searches at airports would prevent people from boarding planes with weapons, but at too high a cost.
- Whatever the justification for the intrusion, if there are less intrusive means of achieving the same end at a reasonably comparable cost, the less intrusive means ought to be preferred. There is no reason to erode Americans' privacy when equivalent results can be achieved without doing so.
- Any new system developed and implemented must be designed to be tolerable in the long term. The war against terror, uniquely, is one with no immediately foreseeable end. Thus, excessive intrusions may not be justified as emergency measures that will lapse upon the termination of hostilities. Policymakers must be restrained in their actions; Americans might have to live with their consequences for a long time.

From these general principles can be derived certain other more concrete conclusions regarding the development and construction of any new technology:

- No new system should alter or contravene existing legal restrictions on the government's ability to access data about private individuals. Any new system should

mirror and implement existing legal limitations on domestic or foreign activity, depending upon its sphere of operation.

- Similarly, no new system should alter or contravene existing operational system limitations. Development of new technology is not a basis for authorizing new government powers or new government capabilities. Any such expansion should be independently justified.
- No new system that materially affects citizens' privacy should be developed without specific authorization by the American people's representatives in Congress and without provisions for their oversight of the operation of the system.
- Any new system should be, to the maximum extent practical, tamper-proof. To the extent the prevention of abuse is impossible, any new system should have built-in safeguards to ensure that abuse is both evident and traceable.
- Similarly, any new system should, to the maximum extent practical, be developed in a manner that incorporates technological improvements in the protection of American civil liberties.
- Finally, no new system should be implemented without the full panoply of protections against its abuse. As James Madison told the Virginia ratifying convention, "There are more instances of the abridgment of the freedom of the people by gradual and silent encroachments of those in power than by violent and sudden usurpations."

THE SCOPE OF THE TERRORIST THREAT

The full extent of the terrorist threat to America cannot be fully known. Consider, as an example, one domestic aspect of that threat—an effort to determine precisely how many al-Qaeda operatives are in the United States at this time and to identify those who may enter in the future – a question plainly of relevance to any consideration of CAPPS II or TIA.

Although the estimates of the number of al-Qaeda terrorists in the United States have varied since the initial attack on September 11, the figure provided by the government in recent, supposedly confidential briefings to policymakers is 5,000. This 5,000-person estimate may include many who are engaged in fundraising for terrorist organizations and others who were trained in some fashion to engage in jihad, whether or not they are actively engaged in a terrorist cell at this time. But these and other publicly available statistics support two conclusions: (1) no one can say with much certainty how many terrorists are living in the United States, and (2) many who want to enter in the foreseeable future will be able to do so.

Understanding the scope of the problem demonstrates the difficulty of assessing the true extent of the risk to the United States. Consider this revealing statistic: "[M]ore than 500 million people [are] admitted into the United States [annually], of which 330 million are non-citizens." Of these:

- Tens of millions arrive by plane and pass through immigration control stations, often with little or no examination.

- 11.2 million trucks enter the United States each year. Many more cars do so as well: More than 8.5 million cars cross the Buffalo–Niagara bridges each year alone, and only about 1 percent of them are inspected.
- According to the Department of Commerce, approximately 51 million foreigners vacationed in the United States last year, and this figure is expected to increase to 61 million in three years.
- There are currently approximately 11 million illegal aliens living in the United States. Roughly 5 million entered legally and simply overstayed their lawful visit.
- Over half a million foreign students are enrolled in American colleges, representing roughly 3.9 percent of total enrollment, including:
    1. 8,644 students from Pakistan.
    2. A total of 38,545 students from the Middle East, including 2,216 from Iran, 5,579 from Saudi Arabia, and 2,435 from Lebanon, where Hezballah and other terrorist organizations train.
    3. About 40,000 additional students from North African, Central and Southeast Asian nations where al-Qaeda and other radical Islamic organizations have a strong presence.

This, of course, is only part of the story. The other aspect of the danger to America is the new and unique nature of the threat posed by terrorists. Virtually every terrorism expert in and out of government believes there is a significant risk of another attack. . As last week's truck bombing of Western compounds in Saudi Arabia reminds us, unlike during the Cold War, the threat of such an attack is asymmetric. In the Cold War era, U.S. analysts assessed Soviet capabilities, thinking that their limitations bounded the nature of the threat the Soviets posed. Because of the terrorists' skillful use of low-tech capabilities (e.g. box cutters and truck bombs) their capacity for harm is essentially limitless. The United States therefore faces the far more difficult task of discerning their intentions. Where the Soviets created "things" that could be observed, the terrorists create only transactions that can be sifted from the noise of everyday activity only with great difficulty. There can, therefore, be little doubt of the importance of research to better understand the value (or lack thereof) of sifting this mass of data. It is a problem of unprecedented scope, and one whose solution is imperative if American lives are to be saved.

As I said at the outset, these considerations of principle and the scope of the threat, while useful in constructing an *ex ante* heuristic for assessing new programs, are only of real value in application to concrete problems and proposed solutions. Whenever I speak on this topic, I always emphasize (as I do here today) that specifics matter. It is not enough to condemn every governmental initiative. Nor is it apt to afford the government a blank check for all actions designed to repel terror. Rather, each program and proposal must be carefully assessed on its own individual merits.

"Data Mining" -- Total Information Awareness Today

To that end, let me first discuss the concept of data mining and more particularly the Total Information Awareness program ("TIA") – a program that has been widely

misunderstood. [For more detail on the program I refer you to a paper I co-authored with my Heritage colleague, Michael Scardaville – "The Need to Protect Civil Liberties While Combating Terrorism: Legal Principles and the Total Information Awareness Program," The Heritage Foundation, Legal Memorandum No. 6 (February 2003).]

DATA ANALYSIS

First, and foremost, I think that much of the public criticism has obscured the fact that TIA is really not a single program. Virtually all of the attention has focused on the data mining aspects of the research program – but far more of the research effort is being devoted to providing tools for enhanced data analysis. In other words, TIA is not, as I understand it, about bypassing existing legal restrictions and providing governmental agencies with access to new and different domestic information sources. Rather, it is about providing better tools to enable intelligence analysts to more effectively and efficiently analyze the vast pool of data already at their disposal – in other words to make our analysts better analysts. These tools include, for example, a virtual private network linking existing counter-terrorism intelligence agencies. It would also include, for example, research into a machine translation capability to automatically render Arabic into English. While these developments certainly pose some threat to civil liberty because any enhancement of governmental capability is inherently such a threat, they are categorically different than the data mining techniques that most concern civil libertarians. The threat to civil liberty is significantly less and the potential gain from their development is substantial.

Thus, my first concrete recommendation to you is to not paint with too broad a brush – the distinction between collection and analysis is a real and important one that, thus far, Congress has failed to adequately recognize. Earlier this year, Congress passed an amendment, the so-called Wyden amendment, which substantially restricts TIA development and deployment. That restriction applies broadly to all programs under development by DARPA. That's a mistake. The right answer is not for Congress to adopt a blanket prohibition. Rather, Congress should commit to doing the hard work of digging into the details of TIA and examining its operation against the background of existing laws and the existing terrorist threats at home and abroad.

We have already seen some of the unintended but pernicious effects of painting with such a broad brush. Recently at a forum conducted by the Center for Strategic Policy, DARPA officials discussed how the Wyden amendment had short-circuited plans to sign a Memorandum of Understanding (MOU) with the FBI. The FBI, as this Subcommittee knows, is substantially behind the technological curve and is busily engaged in updating its information technology capabilities. The MOU under consideration would have enabled the FBI to join in the counter-terrorism Virtual Private Network (VPN) being created by the TIA program. Again, the VPN is not a new data collection technology – it is a technology to enhance data analysis by allowing information sharing. Other counter-terrorism agencies with exclusively foreign focus are already part of the VPN – the CIA and DIA for example. Though the Department of Defense has not reached a final interpretation of the Wyden amendment, the lawyers at DoD were sufficiently concerned with its possible scope that they directed DARPA to not sign the MOU with the FBI. As a consequence one of our principal domestic counter-terrorism agencies is being excluded from a potentially valuable

network of information sharing. Extrapolating from this unfortunate precedent, it is likely that the Wyden amendment will have the effect of further balkanizing our already unwieldy domestic counter-intelligence apparatus. The same law will probably be interpreted to prohibit the Department of Homeland Security from joining the network, as well as the counter-terrorism agencies of the various States.

In short, as Senator Shelby has written of TIA:

> The TIA approach thus has much to recommend it as a potential solution to the imperative of deep data-access and analyst empowerment within a 21st-century Intelligence Community. If pursued with care and determination, it has the potential to break down the parochial agency information "stovepipes" and permit nearly pure *all* source analysis for the first time – yet without unmanageable security difficulties. If done right, moreover, TIA would be infinitely scalable: expandable to as many databases as our lawyers and policymakers deem to be appropriate.
>
> TIA promises to be an enormously useful tool that can be applied to whatever data we feel comfortable permitting it to access. How broadly it will ultimately be used is a matter for policymakers to decide if and when the program bears fruit. It is worth emphasizing, however, that TIA would provide unprecedented value-added even if applied exclusively *within* the current Intelligence Community – as a means of finally providing analysts deep but controlled and accountable access to the databases of collection and analytical agencies alike. It would also be useful if applied to broader U.S. Government information holdings, subject to laws restricting the use of tax return information, census data, and other information. Ultimately, we might choose to permit TIA to work against some of the civilian "transactional space" in commercially-available databases that are already publicly and legally available today to marketers, credit card companies, criminals, and terrorists alike. The point for civil libertarians to remember is that policymakers can choose to restrict TIA's application however they see fit: it will be applied only against the data-streams that our policymakers and our laws permit.

Put more prosaically, it remains for this Congress to decide how widely the analytical tools to be provided by TIA are used – but it is imperative that Congress understand that the tools themselves are distinct from the databases to which they might have access.

DATA COLLECTION – STRUCTURAL LIMITATIONS

As for concerns that the use of new data collection technologies could intrude on civil liberties by affording the government access to new databases, I certainly share those concerns. The question then is how best to ensure that any domestic use of TIA (or, frankly, any other intelligence gathering program) does not unreasonably intrude on American domestic civil liberties. There are several operational principles that will effectively allow the use of TIA while not substantially diminishing American freedom. Amongst these are the following requirements:

Require congressional authorization. In light of the underlying concerns over the extent of government power, it is of paramount importance that there be formal congressional consideration and authorization of the TIA program, following a full public debate, before the system is deployed. Some of the proposed data-querying methods (for example, the possibility for access to non-government, private databases, which is discussed in the next section) would require congressional authorization in any event. But, more fundamentally, before any program like TIA—with both great potential utility and significant potential for abuse—is implemented, it ought to be affirmatively approved by the American people's representatives. Only through the legislative process can many of the restrictions and limitations suggested later in this testimony be implemented in an effective manner. The questions are of such significance that they should not be left to executive branch discretion alone.

Maintain stringent congressional oversight. In connection with the congressional authorization of TIA, Congress should also commit at the outset to a strict regime of oversight of the TIA program. This would include periodic reports on TIA's use once developed and implemented, frequent examination by the U.S. General Accounting Office, and, as necessary, public hearings on the use of TIA. Congressional oversight is precisely the sort of check on executive power that is necessary to insure that TIA-based programs are implemented in a manner consistent with the appropriate limitations and restrictions. Without effective oversight, these restrictions are mere parchment barriers. While potentially problematic, one can be hopeful that congressional oversight in this key area of national concern will be bipartisan, constructive, and thoughtful. Congress has an interest in preventing any dangerous encroachment on civil liberties by an executive who might misuse TIA.

My colleagues at The Heritage Foundation have written extensively on the need for reorganization of the congressional committee structure to meet the altered circumstances posed by the war on terrorism and the formation of the Department of Homeland Security. Oversight of any program developed by TIA would most appropriately be given either to the committee which, after reorganization, had principal responsibility for oversight of that Department or, if TIA is limited to foreign intelligence applications, to the two existing intelligence committees.

Construct TIA to permit review of its activities. To foster the requisite oversight and provide the American public with assurances that TIA is not being used for inappropriate purposes, the TIA program must incorporate, as part of its basic structure, an audit trail system that keeps a complete and accurate record of activities conducted using the technology. To the maximum extent practical, the audit system should be tamper-proof. To the extent it cannot be made tamper-proof, it should be structured in a way that makes it evident whenever anyone has tampered with the audit system. Only by providing users, overseers, and critics with a concrete record of its activity can TIA-developed technology reassure all concerned that it is not being misused.

Limit the scope of activities for which queries of domestic non-government databases may be used. TIA is a technological response to the new, significant threat of terrorism at home and abroad. After September 11, no one can doubt that domestic law

enforcement and foreign intelligence agencies face a new challenge that poses a qualitatively greater threat to the American public than any other criminal activity.

U.S. foreign counterintelligence efforts are responding to a new and different form of terrorism and espionage. It is appropriate, therefore, that the use of TIA to query non-government databases be limited to the exigent circumstances that caused it to be necessary. Technology being developed for TIA to build models, query and correlate data, and uncover potential terrorist activity should be used (whether for law enforcement or intelligence purposes) only to investigate terrorist, foreign intelligence, or national security activities, and the TIA technology should never be used for other criminal activity that does not rise to this level.

It is important to be especially wary of "mission creep," lest this new technology become a routine tool in domestic law enforcement. It should not be used to fight the improperly named "war on drugs," combat violent crime, or address other sundry problems. While certainly issues of significant concern, none of these are so grave or important as the war on terrorism. Given the *bona fide* fears of increased government power, any systems that might be derived from TIA should be used only for investigations where there is substantial reason to believe that terrorist-related activity is being perpetrated by organizations whose core purpose is domestic terrorism.

The legislation authorizing TIA should enact this limitation. Congress should, therefore, specify that use of the TIA system is limited to non-government data inquiries that are certified at a sufficiently high and responsible level of government to be necessary to accomplish the anti-terrorism objectives of the United States. Only if, for example, a Senate-confirmed officer of the Department of Justice, Homeland Security, FBI, or CIA (such as an Assistant Attorney General or the FBI Director) certifies the objectives of the query based upon a showing of need should one be made.

Limit access to the results of the search. A corollary to the need to limit authority to initiate an analysis using TIA is an equivalent necessity to limit access to the findings of any resulting analysis. It would be unacceptable, for example, for the data and analysis derived from a TIA query (or, for that matter, a CAPPS II query), and linked to an individual identity, to be available to every Transportation Security Administration screener at every airport. Assuredly, after high-level analysis substantiated the utility of the information, it could be used to create watch lists and other information that can be shared appropriately within the responsible agencies. Until that time, however, access to the results of a TIA search should be limited by the authorizing legislation to a narrow group of analysts and high-level officials in those intelligence, counterintelligence, and law enforcement agencies.

Distinguish between use of TIA in examining domestic and foreign activities. In practice, it will be possible to use whatever technology the TIA program develops to unearth terrorist activity or conduct counterintelligence activity both abroad and domestically. Existing law places significant restrictions on intelligence and law enforcement activity that addresses the conduct of American citizens or occurs on American soil. Conversely, fewer restrictions exist for the examination of the conduct of non-Americans abroad.

The development of TIA is not a basis for disturbing this balance and changing existing law. Thus, even if Congress ultimately chooses to prohibit the implementation of TIA for any domestic law enforcement purpose whatsoever (a decision that would be unwise), it would be a substantial *expansion* of existing restrictions on the collection of foreign intelligence data were it to extend that prohibition to use of the technology with respect to overseas databases containing information on non-citizens. At a minimum, in considering TIA, Congress should ensure that, consistent with existing law, any program developed under TIA will be used in an appropriate manner for foreign intelligence and counterintelligence purposes.

Impose civil and criminal penalties for abuse. Most important, all of these various prohibitions must be enforceable. Violations of whatever prohibitions Congress enacts should be punishable by the executive branch through its administrative authority. Knowing and willful violations should be punishable as crimes. These forms of strong punishment are a necessary corollary of any TIA authorization.

In addition, Congress should enlist the third branch of government—the courts—to serve as a further check on potential abuse of TIA. As is detailed below, the courts will be involved in challenges to TIA information requests. To insure effective oversight of the use of TIA by the courts, Congress should also authorize a private right of civil action for injunctive relief, attorneys' fees, and (perhaps) monetary damages by individuals aggrieved by a violation of the restrictions Congress imposes.

Sunset the authorization. Any new law enforcement or intelligence system must withstand the test of time; it must be something that the American public can live with, since the end of the war on terrorism is not immediately in sight. Congress should be cautious, therefore, in implementing a new system of unlimited duration. It is far better for the initial authorization of TIA to expire after a fixed period of time so that Congress may evaluate the results of the research program, its costs (both public and private), and its long-term suitability for use in America. A sunset provision of five years would be ample time for Congress to gather concrete information on the program. With such information, Congress will be in a position to continue, modify, or terminate the program, as it deems appropriate.

DATA COLLECTION – LEGAL LIMITATIONS

As I noted earlier, the existing legal structure and the overarching principles that I see in American law lead to a singular legal recommendation for the structure and operation of TIA:

> *TIA should be implemented only in a manner that mirrors existing legal restrictions on the government's ability to access data about private individuals—nothing more and nothing less.*

This recommendation may be particularized in the following ways:

TIA should not have access to protected governmental databases. Most government databases (e.g., arrest records and driver's licenses) contain information about an individual that is accessible to the government and in which the individual has no reasonable expectation of privacy. Linking such information through TIA technology should

not be subject to any greater restriction than that applied to its initial inclusion in the local, state, or federal government database from which the information is retrieved. By contrast, some existing governmental databases (like the Census database) cannot be used for purposes other than those for which they were created. Others (like the IRS database on taxpayer returns) can be accessed only with a special court order.

In authorizing the development of TIA technology, Congress should make it clear that information from existing government databases may be queried using TIA structured query programs only to the extent that the government already lawfully has access to the data. The creation of TIA-based networks should not be viewed as an excuse or opportunity to remove existing restrictions on the use of particularly sensitive individual data.

Information from private domestic databases should be accessed only after notice to the data holder. A similar limitation should also apply to queries made of private, non-government databases from which the government seeks information. Where predication for an investigation (whether criminal or foreign intelligence) exists, law enforcement or intelligence authorities should have the ability to secure data about an individual or pattern of conduct from private databases just as they do under current law.

Thus, with appropriate predication and/or court authorization (if the law requires), the government should be able to secure data from banks, credit card companies, and telephone companies about the conduct of specified individuals or about specified classes of transactions. But existing warrant and subpoena requirements should not be changed. Such data gathering should be done only at the "retail" level when a particularized basis for investigation exists.

More important, in each instance where data is sought from a private database, the holder of the data should be notified prior to securing the data and (as in the context of a subpoena today) have the capacity to interpose an objection to the data query to the same extent the law currently permits. The law today does not provide a mechanism by which such information requests may be made other than by subpoena. Thus, in authorizing a TIA-based investigative system, Congress should require that any aspects of TIA seeking data from private databases should operate in a manner similar to that in contemporary subpoena practice.

As this analysis makes evident, one should strongly oppose any effort to incorporate in TIA the ability to gather private database information at the "wholesale" level (e.g., all bank transactions processed by Citibank). One should also strongly oppose any TIA-based system that allows access to privately held data without notice to (and the opportunity to object by) the data holder. In short, the development of TIA technology and the war on terrorism is not a justification for the routine incorporation of all private data and information in a single government database.

TIA is not a justification for creating new government databases. Given the clear distinction that the law enacts between access to government and access to private, non-government databases, a further cautionary note is in order. In order to evade the legal strictures limiting access to information in private databases, the government might be tempted, in effect, to "institutionalize" the information it deems relevant by enacting new

data-reporting requirements to capture in government databases information that now exists only in private databases to which access is less ready. The first such proposal may already have been made: that Americans flying abroad be required to provide their travel itineraries to the Transportation Security Administration upon their departure from America.

The expansion of existing government databases should be resisted except upon a showing of extraordinary need. The government already collects too much information about Americans on a day-to-day basis. While many government programs require the collection of such data to permit them to operate, one should not create databases where no program requiring their creation exists—otherwise, there is the risk of wholesale evasion of existing legal restrictions on the use of information in private databases. Initiatives such as the new itinerary-collection program should be evaluated independently to determine their necessity and utility.

There must be absolute protection for fundamental constitutionally protected activity. The gravest fear that most Americans have about TIA is that it might be used to transmit queries about and assemble dossiers of information on political opponents. One should not discount these fears as they rest on all-too-recent abuses of governmental power. If a system developed based on TIA technology is used to enable an effort to harass anti-war demonstrators or gather information on those who are politically opposed to the government's policies (as the FBI used its investigative powers to do in the 1960s and 1970s), such abuse should be terminated immediately.

This prospect is not, however, sufficient to warrant a categorical rejection of all of the benefits to the war on terrorism that TIA technology might provide. TIA can be developed without these abuses, and aspects of the technology under investigation in fact hold the promise of enhancing civil liberties. Still, it is imperative that any implementing legislation has concrete, verifiable safeguards against the misuses of TIA. These should include, for example, an absolute prohibition on accessing databases relating to support of political organizations that propagate ideas—even ones favorable to terrorist regimes—absent compelling evidence that the organizations also aid terrorist conspirators with monetary, organizational, and other support not protected by the First Amendment. There must be an absolute prohibition on accessing databases relating solely to political activity or protest.

TIA should build privacy protections into its architecture. Finally, it should be recognized that access to data is not necessarily equated with a loss of privacy. To be sure, it may in many instances amount to the same thing, but it need not. There is, for example, a sense in which the automated screening of personal data by computer enhances privacy: It reduces the arbitrariness or bias of human screening and insures that an individual's privacy will be disrupted by human intervention only in suspicious cases.

In addition, those developing TIA can be required to construct a system that initially disaggregates individual identifiers from pattern-based information. Only after the pattern is independently deemed to warrant further investigation should the individual identity be disclosed. So, for example, only after a query on the bulk purchase of the precursors of Ricin poison turned up a qualifying series of purchases linked to a single individual would the individual's name be disclosed to terrorism analysts.

Thus, everyone on both sides of the discussion should welcome one aspect of TIA, the Genisys Privacy Protection program. The Genisys program is developing filters and other protections to keep a person's identity separate from the data being evaluated for potential terrorist threats. In authorizing TIA, Congress should mandate that a trusted third party rather than an organization's database administrator control these protections.

CAPPS II

Virtually all of what I have said about TIA, is equally valid in any consideration of the Computer Assisted Passenger Prescreening System (CAPPS II), which has, of course, already been authorized by Congress. In particular, the TSA's new program should be:

- Constructed to include an audit trail so that its use and/or abuse can be reviewed;
- Not be expanded beyond its current use in identifying suspected terrorists and threats to national security – it should not be used as a means, for example, of identifying drug couriers or deadbeat dads;
- Sunset after a fixed period of time, thereby ensuring adequate Congressional review;
- Prohibited from having access to any protected government databases, like the Census; and
- Have significant civil and criminal penalties for abuse.

The basis for these recommendations is, essentially, the same analysis I have already laid out with respect to TIA, and I will not burden the record by repeating it here.

There are, however, several aspects of the CAPPS II program that warrant additional commentary because they pose issues of concern:

Access to Data. First, if CAPPS II is to be effective, my recommendation that access to the results of a data inquiry be limited will need to be revisited. The very hallmark of CAPPS II is the idea that some form of "result" will necessarily be immediately available to TSA screeners on a "real-time" basis so that they can make near-instantaneous decisions regarding whom to screen or not screen prior to allowing passengers to board the aircraft. If CAPPS II were designed so that detailed personal information on each passenger were transmitted to every TSA screener, I would think that the architecture of the system did not adequately protect individual privacy. Thus, in my view, the analysis passed by the CAPPS II system to TSA employees at the airport must be limited to a reported color code – red, yellow or green – and should not generally identify the basis for the assignment of the code. My understanding is that this is the current intent of those developing CAPPS II and that intent should be implemented.

Privacy. It is worth noting that CAPPS II precisely reverses the privacy protection equation being developed in the context of TIA. To protect privacy, the TIA program plans

to disaggregate analysis from identity by making the data available to the analyst while concealing the identity of the subject of the inquiry unless and until disclosure is warranted. In the reverse of this paradigm, CAPPS II will disclose the identity of the potential threat (through a red/yellow/green system displayed to the screener, warning of a particular individual) but will conceal from the screener the data underlying the analysis – again, until such time as a determination is made that the two pieces of information should be combined. The privacy protection built into CAPPS II is therefore the mirror image of the system contemplated for TIA. It is by no means clear which method of protecting privacy is *ex ante* preferable – but it is clear that the two systems operate differently and if we are to have any sort of CAPPS II system at all, it can only have privacy protections of the second kind.

One other brief point should be made about privacy – in many ways the implementation of CAPPS II is not an unalloyed diminution of privacy. Rather it is the substitution of one privacy intrusion (into electronic data) for another privacy intrusion (the physical intrusiveness of body searches at airports). Similarly, the use of CAPPS II may reduce the need for random searches and eliminate the temptation for screeners to use objectionable characteristics of race, religion, or national origin as a proxy for threat indicators.

Here one cannot make broad value judgments – each person weighs the utility of their own privacy by a different metric. But I do venture to say that for many Americans, the price of a little less electronic privacy might not be too great if it resulted in a little more physical privacy, fewer random searches, and a reduction in invidious racial profiling.

Domestic Use of CAPPS II. The distinction earlier drawn between foreign and domestic applications of TIA is simply inapposite to any consideration of CAPPS II. By its nature, if it is to be at all effective, CAPPS II must at least operate domestically – that is where the gravest threat exists. Permitting the domestic use of factual data analysis systems requires, of course, a value judgment – one that Congress is uniquely capable of making. For my own part, I do not perceive the necessity of domestic operation as precluding the implementation of a suitably narrow inquiry system – but I do note the issue so that you may form your own judgments.

Government Databases. I mention this issue not because any particular aspect of the CAPPS II program presents an immediate concern – TSA has made it clear that it will not use CAPPS II to create a new government database – but simply as a cautionary note. Though such plans do not exist now, the creation of a government database of domestic travelers might, in the future, prove tempting. We should acknowledge that temptation at the outset and consciously and firmly reject it. The only information the government should ever retain about individuals who are screened and permitted to proceed under "green" or "yellow" cards is information sufficient to respond to an individual challenge to an analysis listing that individual as a potential risk.

Non-Government Databases. Next, we must consider the issue of access to non-government commercial databases. In general, the non-government databases to which CAPPS II will have access are databases whose holders make their data generally

available to all members of the public (sometimes, as in the Yellow Pages, for free; in other circumstances, for a fee). As a general matter, rules for new programs like CAPPS II relating to government access to data should mirror existing legal restrictions on the government's ability to access data about private individuals -- nothing more and nothing less. Thus, since the government may now have access to such public, non-government databases without any notice to or approval of either the data holder or the subject of the data inquiry, I see no significant privacy concern in affording access to that information through the CAPPS II system.

I should hasten to add, however, that some of the databases to which CAPPS II might seek access are *private* non-government databases, to which the public does not have general access – for example, credit card use information. In some instances access to this information may be the lynchpin of the system, enabling identification of an individual with a high degree of certainty. As with my recommendations regarding TIA, CAPPS II should not generally be allowed to query such databases without first providing notice to the data holder and mechanism by which the data holder may object to the query and seek a judicial determination of the objection. If it is concluded that CAPPS II will routinely require access to a specific class of such private data, it may be appropriate for Congress to consider a blanket authorization of such access – but only after it deems the utility of CAPPS II sufficiently great to warrant that step. In addition there is one obvious exception to this rule – and one that is necessary if CAPPS II is to function at all: It is a tautological necessity that, in order to function, CAPPS II will need access to the normally private data contained in airline reservation systems themselves.

Protection of Constitutional Liberties. Finally, the unique subject matter of the CAPPS II system calls for heightened sensitivity to the potential for an infringement on protected constitutional liberties. I have generally been supportive of the potential inherent in the development of the TIA system. In part, that reflects my belief in the benefits of technology. But it also reflects my conviction that existing Supreme Court precedent, dating back to the 1960s, accurately captures the scope of the Constitutional privacy protection embodied in the Fourth Amendment: The Constitution affords no additional protection to information that an individual has made available to other individuals or institutions. Privacy concerns relating to the further distribution of such information are matters of policy and legislative concern, not constitutional law.

By contrast, CAPPS II implicates at least two fundamental liberty interests guaranteed by the Constitution. Most obviously, since the 1960s the Constitution has recognized a fundamental right to travel – indeed, one might reasonably say that one significant purpose of the Federal union was to insure the freedom of commerce and travel within the United States. Second, many of the indicators that *might* be used to identify potential terrorists are also indicators that, in other circumstances, are potentially the products of protected First Amendment activity – in other words, though CAPPS II is not intended to impinge upon free political speech, it may have the collateral effect of doing so.

Thus, there is a significant risk that a mal-administered system will impinge upon fundamental constitutional liberties. I am not, however, one to say that the risk of such impingement should result in abandonment of the program – especially not in light of the

potentially disastrous consequences of another terrorist attack in the United States. I do, however, believe that some fairly stringent steps are necessary to provide the requisite safeguards for minimizing inadvertent infringements of civil liberty in the first instance and correcting them as expeditiously as possible. Those steps would include some or all of the following:

- The use of CAPPS II should be subject to extensive, continuous Congressional oversight. By this I do not mean the mere reporting of raw data and numbers – I mean that, at least as a spot check, Congress should examine individual cases (if necessary using confidential procedures to maintain classified status) to assure itself that the CAPPS II methodology is not being misused. In other words, the database contemplated by the CAPPS II system for "positives" (i.e. red cards) should, under classified circumstances, be subject to Congressional scrutiny;
- The "algorithm" used to screen for potential danger must, necessarily, be maintained in secret, as its disclosure would frustrate the purpose of CAPPS II. It must, however, also be subject to appropriate congressional scrutiny in a classified setting;
- An individual listed for additional screening or prohibited from flying should be entitled to know the basis for his or her listing and should have a mechanism for challenging the listing before a neutral arbiter or tribunal. To the extent practicable the review should be as prompt as possible;
- Because commercial databases may be error-ridden, no American should be totally denied a right to travel (i.e. red-carded) and subject to likely arrest as a suspected terrorist solely on the basis of public, commercial data. An indication of threat sufficient to warrant denial of that right should (except in extraordinarily compelling circumstances) be based only upon significant intelligence from non-commercial sources.
- The CAPPS II system should be designed so that the No-Fly/Red Card designation, though initially made as the product of a computer algorithm, is never transmitted to the "retail" TSA screening system until it has been reviewed and approved by an official of sufficiently high authority within TSA to insure accountability for the system. Nor, as I've said, is there any reason for the underlying data ever to be transmitted to the TSA screener.

* * * * *

Mr. Chairman, thank you for the opportunity to testify before the Subcommittee. I look forward to answering any questions you might have.

Mr. PUTNAM. Thank you very much, particularly for your respect for the time limit.

Our next witness is Barry Steinhardt. Mr. Steinhardt has served as associate director, American Civil Liberties Union for the past 10 years. He was recently named as inaugural director, ACLU Program on Technology and Liberty. Mr. Steinhardt was a co-founder of the Global Internet Liberty Campaign, the world's first international coalition of non-governmental organizations concerned with the rights of Internet users to privacy and free expression. He is a member of the Advisory Committee to the U.S. census and the Blue Ribbon Panel on Genetics of the National Conference of State Legislatures. He was a member of the U.S. delegation to the recent G8 Government and Private Sector Tokyo Conference on Cybercrime. He is a 1978 graduate of Northeastern University School of Law.

Welcome.

Mr. STEINHARDT. Thank you, Mr. Chairman and members of the committee, for the opportunity to testify this morning.

The timeliness of your hearing could not be more apt. The explosion of computers, cameras, sensors and other technologies in the last 10 years has brought us to the edge of surveillance society. The fact is there are no longer any technical bars to the creation of that surveillance society. If we don't take steps to control and regulate surveillance, to bring it into conformity with our values, we will find ourselves being tracked, analyzed, profiled and flagged in our daily lives to the degree we can scarcely imagine today, being forced into an impossible struggle to conform to the letter of every rule, law and societal assumption of correctness. Our transgressions, whether they are real or an imagined product of bad data will become permanent scarlet letters that will follow us through our lives.

We should be responding to this new threat, these new circumstances by building stronger restraints to protect our privacy but instead, we have been weakening those restraints, loosening the regulations. Most ominously we are contemplating the introduction of powerful new surveillance infrastructures that will tie together all this information. The Total Information Program [TIA], and CAPPSII are prime examples of the new infrastructures for surveillance.

DARPA has recently sought to underplay TIA. To my right you will see two charts, both prepared by the Total Information and Awareness Office itself. The first was published before the furor erupted. It makes quite plain the TIA was designed to conduct a massive search through records of 300 million Americans, including financial, education, housing, travel, medical and communications data.

The second, which was prepared after the furor and Congress' passage of the Wyden amendment which prevented DARPA from training TIA on Americans, omits all the original detail and notes that access is "restricted by law." The reality is that the only thing that significantly restricts TIA is the Wyden amendment itself. There is no overarching law that prohibits the Government from gaining or buying access to most of the details of our lives from having what Poindexter calls "total information awareness."

Our memo outlines questions we believe DARPA must answer when it sends to the Congress your mandated report which is due today. Consider those questions as you read the report and insist the report be made public.

CAPPSII is portrayed by the TSA as a more effective and benign successor to CAPPSI Program and the so-called No Fly list. The failure of these programs to protect either our security or our freedoms is well documented. We don't need to look into history to speculate about what the consequences of abuse of that sort of data will be. The No Fly list and the CAPPSI Program demonstrate quite well and there have been literally hundreds of communications with Members of Congress that forwarded to TSA and recently revealed under a Freedom of Information Act request.

The ACLU has six questions which we urge the Congress to ask about CAPPSII. The questions range from its cost to its fundamental fairness to how do innocent civilians correct mistakes made in secret or are we deemed to repeat the failure of the No Fly list. Let me highlight two questions for you. First, and I would suggest this is the first question that should be asked about any security measures, will it work? Will we really be able to pick out a few terrorists among 100 million Americans who fly? We urge you to heed the advice of Mark Forman of the Office of Management and Budget who told this very subcommittee "If we can't prove it lowers risk, it is not a good investment for government."

Citing the obvious problems of error, if you stop and think about it for a moment, even at 99.9 percent accuracy rate among the 100 million Americans who fly every year, would result in 100,000 errors each year. The problem with CAPPSII is that profiles are always one step behind the attackers. The spokesperson for DHS recently said "One thing we know about terrorists is there is no way to predict what will happen."

The second question is what will be the cost to our freedom of building a system like this? It is historical fact that government agencies and surveillance systems alike tend to expand and not contract, the phenomenon known as mission creep. Can we really restrict CAPPSII to its original purpose? How long before it is extended to cover our entire transportation sector as Admiral Loy has suggested it might, how long before the system is expanded to reach more and more sectors of our economy and society, how long before the data which we are told now is not going to be retained will be retained? How long before CAPPSII becomes the Total Information Program?

Your subcommittee is performing an essential oversight role in examining these programs and these questions. I urge you to continue to act with vigor and expedition before it is too late to turn back the clock on the looming surveillance society.

Thank you.

[The prepared statement of Mr. Steinhardt follows:]

AMERICAN CIVIL LIBERTIES UNION

WASHINGTON NATIONAL OFFICE
Laura W. Murphy
Director

1333 H Street, NW, 10TH Floor, Washington, DC 20005

Tel (202) 544-1681 Fax (202) 546-0738

STATEMENT OF
BARRY STEINHARDT
DIRECTOR
TECHNOLOGY AND LIBERTY PROGRAM
AMERICAN CIVIL LIBERTIES UNION

ON
GOVERNMENT DATA MINING

BEFORE THE
TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS
SUBCOMMITTEE
OF THE HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT REFORM

MAY 20, 2003

BARRY STEINHARDT
DIRECTOR
TECHNOLOGY AND LIBERTY PROGRAM
AMERICAN CIVIL LIBERTIES UNION

ON
GOVERNMENT DATA MINING

BEFORE THE
TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS SUBCOMMITTEE
OF THE HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT REFORM

MAY 20, 2003

My name is Barry Steinhardt and I am the director of the Technology and Liberty Program at the American Civil Liberties Union (ACLU). The ACLU is a nationwide, non-partisan organization with nearly 400,000 members dedicated to protecting the individual liberties and freedoms guaranteed in the Constitution and laws of the United States. I appreciate the opportunity to testify about government data mining on behalf of the ACLU before the Technology, Information Policy, Intergovernmental Relations And The Census Subcommittee of the House of Representatives Committee on Government Reform.

Drift toward a surveillance society

Government data mining is a vital topic because it is representative of a larger trend that has been underway in the United States: the seemingly inexorable drift toward a surveillance society – a trend well documented in a recent cover story in the *New York Times Magazine* and another in MIT's *Technology Review*.[1]

The explosion of computers, cameras, sensors, wireless communication, GPS, biometrics, and other technologies in just the last 10 years is feeding what can be described as a surveillance monster that is growing silently in our midst. Scarcely a month goes by in which we don't read about some new high-tech method for invading privacy, from face recognition to implantable microchips, data-mining to DNA chips, and RFID identity chips in our clothing. The fact is, there are no longer any *technical* barriers to the creation of the surveillance society.

While the technological bars are falling away, we should be strengthening the laws and institutions that protect against abuse.

Unfortunately, even as this surveillance monster grows in power, we are weakening the legal chains that keep it from trampling our privacy. We should be responding to intrusive new technologies by building stronger restraints to protect our privacy; instead, we are doing the opposite – loosening regulations on government surveillance, watching passively as private

---

[1] Matthew Brzezinski, "Fortress America," *New York Times Magazine*, Feb. 23 2003; Dan Farmer and Charles C. Mann, "Surveillance Nation," *Technology Review*, April 2003 and May 2003.

surveillance grows unchecked, and contemplating the introduction of tremendously powerful new surveillance infrastructures that will tie all this information together. (The ACLU has written a report on this subject, entitled *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, which is available on our Web site at www.aclu.org/privacy.)

Combating illusions of security

Given this larger context in which data-mining proposals are being proposed, Congress must proceed carefully before authorizing their use and certainly none should be built or implemented without your explicit authorization.

In exercising your responsibilities, we believe you and all policymakers should apply a two-step test to proposals for potentially intrusive new programs and technologies:

1) Does the program actually makes us safer?
2) Is the actual improvement in safety provided by a technology enough to counterbalance its cost to our privacy and other fundamental freedoms?

If a new program is not actually effective, the matter should end there. There is no need to engage in detailed balancing tests or evaluations of a program's effect on privacy if it is not going to increase security.

We are not opposed to effective security. Far from it – as a New Yorker whose office is less than a dozen blocks away from the World Trade Center site, I take security especially seriously. And the ACLU has been calling for improvements in airport security since at least 1996, when we proposed measures like improved training and screening of airline personnel, tighter control of access to secure areas in airports, measures to enforce security standards at foreign airports, and luggage matching (recognized around the globe as a basic component of airline security, which the US has still failed to impose).[2] We have also proposed affirmative steps to increase the effectiveness of U.S. intelligence agencies at combating terrorism, including more reliance on human sources, better utilization of existing information technology to "connect the dots," provision of sufficient incentives to recruit a diverse and skilled workforce of intelligence analysts (especially those skilled in foreign languages), in-depth training of all national security personnel, and a thorough review of excessive secrecy (it is secrecy, not civil liberties, which almost certainly represents the greatest barrier to effective information sharing in the government today).[3]

What we do oppose are measures that offer nothing but the illusion of security – programs that make us no safer but carry a substantial price in lost freedom.

---

[2] See for example, Statement Of Gregory T. Nojeim Before White House Commission On Aviation Safety And Security, September 5, 1996, online at http://archive.aclu.org/congress/airtest.html; or Statement Of Gregory T. Nojeim Before International Conference On Aviation Safety And Security In The 21st Century, January 14, 1997, online at http://archive.aclu.org/congress/t011497a.html.

[3] Timothy Edgar, Testimony at a Hearing on "Securing the Freedom of the Nation: Collecting Intelligence Under the Law" Before the House Permanent Select Committee on Intelligence, April 9, 2003, online at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12313&c=206.

Total Information Awareness
The Pentagon's "Total Information Awareness" (TIA) program is a good example of a fundamentally flawed system that will not be effective at increasing our security.

DARPA has offered repeated assurances that it is only the developer of this system, and will not itself be involved in its deployment, and we take them at their word. TIA officials, however, appear to be understating what they have in mind. When their recent statements explaining the program are compared to statements made before TIA exploded as a controversy in the media, the story appears to have changed. For example, a chart that was posted on the TIA Web site (but replaced after the story broke) contained an extensive list of the categories of information planned for inclusion in the system: Financial, Education, Travel, Medical, Veterinary, Country Entry, Place / Event Entry, Transportation, Housing, Critical Resources, Government, Communications. The chart clearly indicated that such data would be fed into "automated virtual data repositories." (See Appendix 1) This chart has now been replaced by a new, more soothing presentation of what the program would look like. (See Appendix 2) Accompanying the new chart is a new and far less foreboding logo.

The fact is, TIA would be the infrastructure for a massive government surveillance program. In theory, it will be capable of searching countless public and private databases and combining the information found there to create an intimate look into the lives of 300 million Americans. We believe that members of Congress did precisely the right thing when you prohibited DARPA from training TIA on Americans, and required that it report on the key privacy and security issues involving TIA. That report will apparently be sent today. In preparation for that report, the ACLU has prepared its own report detailing the key questions that DARPA must answer to satisfy the Congressional requirement. (See Appendix 3)

Mission Creep
Perhaps the most fundamental problem with a surveillance system like TIA is "mission creep." Information systems inevitably grow – not only in the data they collect, but in the uses to which they are put. My parents, for example, were promised when they received their Social Security numbers that they would not be used as a national identifier. Congress wrote into law a prohibition on their use for any purpose other than administering the retirement program. Fast forward a few decades, and when my children received their Social Security numbers – at birth – they were immediately put to use for a host of identification purposes.

Once TIA is in place, we will see a similar dynamic. Its operators will grow frustrated at the gaps in its coverage, and seek to have more and more transaction records available to them. TIA will be expanded from terrorists to murderers to thieves, and so on down the scale of wrongdoing until everyone is put on guard against the slightest infraction of every law, rule, regulation, and social code in America. At some point the Congress will want to draw the line, but it may well be too late once we start down that track. Despite the promises we are now hearing about protecting privacy – and they are only promises without any real proposals to back them up – TIA is very unlikely to remain restricted to hunting terrorists for very long.

Needed: proof it will work
Where is the proof that TIA's operators will be able to pick out a handful of terrorists among 300 million Americans – that it will actually work?

As the non-partisan Association for Computing Machinery said in a January 23, 2003 letter to the Senate Armed Services Committee:

> Research into areas such as new data mining and fusion methods and privacy-enhancement technologies is needed and welcomed. However, the overall surveillance goals of TIA suffer from fundamental flaws that are based in exceedingly complex and intractable issues of human nature, economics and law. Technological research alone cannot make a system such as TIA viable.
>
> As computer scientists and engineers we have significant doubts that the computer-based TIA Program will achieve its stated goal of "countering terrorism through prevention."

Study after study has concluded that the failure to prevent the 9/11 attacks was a result not of insufficient information, but of the government's inability to process, analyze and distribute the bountiful data it already had.[4] TIA solves the wrong problem: it seeks to prevent terrorism by sucking in vast new troves of information. You don't look for a needle in a haystack by adding more hay to the pile. Especially when much of that hay is rotten – when so much data is wrong, TIA will inevitably be sent on endless wild goose chases, in the process subjecting countless Americans to harassment or worse.

TIA's defenders are fond of noting that it would have to comply with all current laws. But that argument completely misses the point. There are no overarching or specific privacy laws that would fundamentally interfere with the creation or operation of massive data exploitation programs like TIA. Current laws are simply not sufficient to protect our privacy in the face of a program like TIA, which makes use of new technological capabilities that have far outstripped our outdated laws. If not for the Wyden Amendment that restricts the uses of TIA against Americans, it is not clear that anything would have prevented DARPA from building it.

CAPPS II
CAPPS II (for "Computer Assisted Passenger Pre-Screening System") is an attempt to update a more rudimentary airline profiling system already in existence, known as CAPS I. The details of that system, which has been in place for several years, have been kept secret. Transportation Security Agency (TSA) chief Admiral James Loy, however, has said that it is "too broken to be repaired."[5]

---

[4] For example, see *Final Report of the Congressional Joint Inquiry Into September 11: Findings and Conclusions*, online at http://www.fas.org/irp/congress/2002_rpt/findings.html.
[5] Admiral James M. Loy, testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census of the House Committee on Government Reform, May 6, 2003. Loy's prepared statement is online at http://us.gallerywatch.com/testimony/108/pdf/PDFTest2689.pdf. The quotation used here was made during the question-and-answer period.

Another disastrous attempt at airline security has been the government's "no-fly" list of terrorist suspects, ensnaring what appear to be tens of thousands of innocent Americans who find themselves facing intense security scrutiny every time they fly, with no way of finding out how they got on a list or how to get off.

Innocent Americans singled out

Jan Adams and Rebecca Gordon of California, for example, were detained at San Francisco International Airport, and told that their names appeared on the secret "no-fly" list. The two women – peace activists who publish a newspaper called *War Times* – were told nothing about why they were on such a list, or how they could get off. The ACLU has filed suit against the Federal Government on their behalf to find out how the "no fly" lists were created, how they are being maintained or corrected and, most importantly, how people who are mistakenly included on the list can have their names taken off. One question we believe needs answering is whether our clients are on the "no fly" list because of their First Amendment protected political views.[6]

While the Federal Government has thus far refused to provide us with any information, according to documents released to the ACLU by the City of San Francisco, our clients were part of much bigger mess. According to City documents more than 340 persons were investigated by the San Francisco police after being flagged by the "No-Fly List." All of them were eventually found to be innocent of any wrongdoing.

Federal documents obtained by the Electronic Privacy Information Center further confirm that Adams and Gordon are only on the tip of the iceberg.[7] Those documents, which include letters forwarded to the Executive Branch by member of Congress, represent hundreds of complaints by passengers from all walks of life:

- A New Jersey man wrote to his member of Congress because he is routinely denied access to curbside check-in and interrogated at the check-in counter, because his common Middle Eastern name appears on the no-fly list. A former member of the U.S. Navy, the man has never traveled to the Middle East and cannot speak Arabic. "This problem also applies to my son and grandson," he wrote. "Likewise American born, loyal citizens of the United States of America."
- A Washington state man wrote that his co-workers now go out of their way not to be placed on the same reservation as him when traveling. "I have now become known to staff as the person not to travel with," he wrote. Apparently there is nothing he can do to reverse this quasi-pariah status; he was told by Alaska Airlines and Southwest Airlines to contact the government, but has not received responses from any federal agency.
- One woman wrote to the TSA in October 2002 to complain that she, her sister and her 76-year old mother were stopped every time they fly, because their last name

[6] An ACLU press release on the case is online at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12439&c=206

[7] EPIC has posted the documents online at http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html.

> appeared on the no-fly list. "We are from Texas and Oklahoma," she wrote. "Our last name is not foreign. We are not foreign. So why do we get flagged every time?"

Now we are told CAPPS II will fix those problems, but it has all the makings of an even bigger, more frightening system.

CAPPS II: How it would work
As we understand CAPPS II, it is a two-stage program. In the first stage, passengers making a reservation will be asked to provide four pieces of data:

1. name
2. home address
3. home phone number
4. date of birth

This data will be checked against the headers on credit histories and a score will be assigned expressing the likelihood that the person is who she says she is.

In stage 2, secret intelligence and law enforcement databases and potentially commercial databases as well (TSA refuses to rule this out) will be checked, and then, based on a constantly changing algorithm, a security rating will be assigned: green for normal security, yellow for enhanced searches, and red for no-fly.

This proposed system would seem, on its face, to be an improvement over CAPPS I, but both the security and privacy devils are in the details.

First, the identifying information for stage 1 is easily obtained by hook or crook. I bought my own data online for only $29. It is not hard or expensive to assume someone else's identity in the US. Indeed, when I bought my own data, I discovered that there was a second Barry Steinhardt, who apparently lives in California and whose data I could easily obtain for the same $29.

Second, the secret databases, whether governmental or commercial, are likely to be replete with errors that will expose the innocent to humiliation or worse, and waste scarce security resources that could be used far more effectively.

Approximately 100 million Americans fly every year. Since many fly more than once, there are approximately one billion records. If even a tiny fraction of the searches were wrong – let us say 1/10 of 1 percent, or an accuracy rate of 99.9 %, the result would be as many as 1 million erroneous alarms affecting approximately 100,000 separate individuals. That would be unacceptable from a civil liberties point of view – and from a security perspective as well.

And, of course, the underlying records will contain so many inaccuracies that a 99.9% accuracy rate is likely to be unrealistically high. Indeed, while many good people are likely to get caught up in this drag net search, the bad guys will quickly learn how to avoid the system and enhanced security.

The problem with profiling

Although we are not being told how Americans' security ratings will be generated in the secret government databases to which CAPPS II will connect, there is good reason to be suspicious of the whole concept of trying to stop terrorism through profiles.

From a security perspective, profiles are notoriously under inclusive. Those who do not "fit the profile" are given only cursory attention, or no attention at all. Yigal Amir, the man who assassinated Israeli Prime Minister Yitzhak Rabin, did not fit the "profile" of a "terrorist" and was therefore allowed unwarranted access to the Prime Minister. Indeed, the TSA explicitly told us that their CAPPS II profiling would not include a domestic terrorist like Timothy McVeigh, who was convicted of murdering 168 men, women and children in Oklahoma City.

The first recorded bombing of a commercial plane occurred in 1949, when a woman hired assassins to kill her husband, who was on the aircraft. What profile would prevent that from recurring? The first bombing of a U.S. commercial carrier occurred in 1955, when a passenger's son arranged to have a bomb explode in a passenger's luggage so that the son could collect on an insurance policy. Did that passenger fit the profile of a "terrorist?" The problem is that profiles are always one step behind the attackers. Brian Roehrkasse, a spokesperson for DHS Secretary Tom Ridge, could not have put it more clearly when he told USA Today, "One thing that we know about terrorists is there is no way to predict what will happen."[8]

Profiles offend not only the goal of safety, but also the U.S. Constitution. The Fourth Amendment requires that a person should not be subjected to invasive investigative techniques without probable cause that is particularized to that person. Profiling violates that principle: it treats people as potential criminals in the absence of facts specific to them suggesting they are likely to engage in wrongdoing. The use of such stereotypes may temporarily make people feel safer, but they will not actually increase safety and may instead decrease safety. These profiling systems will fail. When they do, the proponents of profiling will not admit that profiling does not work. They will insist that it needs to be "improved" by adding ever more personal data about passengers to the mix. A perfect example of this is CAPPS II itself: Despite the fact that CAPS I is "too broken to be repaired," proponents, rather than giving up on the concept, seek to "improve" it by accessing even more personal information.[9]

The danger of racial profiling

Another danger is that protected characteristics such as race could become the basis for security profiles – and CAPPS II's potential to lead to racial or religious profiling is something that bears just as much advance scrutiny as the issues of privacy and due process.

---

[8] Laura Parker, "Terrorists' most likely weapon here? Bombs," *USA Today*, May 15, 2003.

[9] This was predicted by the ACLU in 1997 and now coming true in 2003. See Statement Of Gregory T. Nojeim Before International Conference On Aviation Safety And Security In The 21st Century, January 14, 1997, online at http://archive.aclu.org/congress/t011497a.html.

As TSA itself has acknowledged, discriminatory profiling is both poor law enforcement technique and offensive to the Constitution. But even profiles that do not explicitly include race or other protected categories as an element can have a discriminatory effect on minority communities. A 1997 Justice Department review of the CAPS I system found that CAPS I did not use race, religion, national origin, or ethnicity as a screening factor, but did find that the system might have a disparate impact on passengers in those groups.[10] The DOJ report included numerous recommendations for oversight and reporting requirements that would ensure that the profiling system remained constitutionally sound. As far as we know, none of these recommendations have been followed to date. For years the ACLU urged the Department of Transportation to establish an independent entity that would monitor abuse in aviation security such as discriminatory searches. The Civil Liberties Advisory Panel to the White House Commission made a similar recommendation.[11] No such panel has been established to date.

Given the secrecy around the CAPPS II risk assessment criteria, it is difficult to assess any likely disparate impact that such a program would have on particular racial, ethnic, or religious groups. But the fact that CAPPS II would rely on credit information suggests individuals without a credit history will immediately be suspect – and that includes the very young, the very old, and especially people of color.

At a minimum, there should be independent assessments of CAPPS II for discriminatory impact before a decision is made to go forward. It is incumbent on the government to ensure that the Constitution's promise of equal protection is not being overrun by ineffective and discriminatory security measures.

Expansion plans already laid

We urge you to heed the advice of Mark Forman, associate director of the Office of Management and Budget, who expressed doubt about CAPPS II in testimony before this very subcommittee in March. "If we can't prove it lowers risk, it's not a good investment for government," he declared, adding that OMB will not let the program go forward until questions about its effectiveness are answered.[12]

But even assuming that CAPPS II could meet the first part of our test (effectiveness), it certainly cannot meet the second. Balanced against any marginal improvement in catching terrorists that the program manages to provide would have to be the fact that it would lead to an enormously dangerous expansion of the government's role. It would none-too-slowly be transformed into a general data mining or profiling system.

Unlike the TIA program, the path has already been explicitly laid out for how CAPPS II will be expanded. As Admiral Loy told this subcommittee on May 6, the TSA envisions CAPPS

[10] Department of Justice Civil Rights Division, October 1, 1997

[11] White House Commission on Aviation Security and Safety, Final Report to President Clinton submitted by Vice President Al Gore, Chairman, February 12, 1997.

[12] Leslie Miller, Associated Press, "U.S. Passenger-Screening Plan Questioned," March 25, 2003.

II being expanded to boats and trains and other modes of transportation, and tied into the massive TSA identity card program known as TWIC (Transportation Workers Identification Credential). Once in place, CAPPS II and TWIC would become the foundation of a "trusted traveler" program, in which the government would begin conducting in-depth background checks on fliers – checks that would be "limited" and "voluntary" at first, but would inevitably spread from there.[13] There are approximately 60 million "frequent flyers" in the US, so this would be no small system.

While we appreciate that Admiral Loy and his staff took the time to meet with us to explain the program and answer some, although not all, of our questions, a system of this size, scope and complexity will inevitably be expanded. As with TIA, mission creep as to both scope and purpose will be unavoidable.

Due process

One of the most troubling aspects of CAPPS II is the absence of any real due process. There will be mistakes and lots of them, but adding a few customer advocates is hardly going to solve the problem, when the individuals still won't be able to get a reason they are on the list, see the information being used against them, or correct errors in their record. Under the TSA's own descriptions of the program, CAPPS II decisions will be based on information contained in government databases that are utterly secret – mysterious black boxes the contents of which we will not know and cannot be revealed to ordinary Americans. For those who are falsely accused, there will be no good way out of the CAPPS II "prison."

In the end, the proponents of CAPPS II have not demonstrated that it will work. Its effectiveness is uncertain, but there is no doubt that it will lay the groundwork for a massive governmental surveillance program.

Questions that Congress should ask about programs like TIA and CAPPS II

In summary, there are six questions that Congress needs to have answered before it should even consider giving a go-ahead to programs like CAPPS II and Total Information Awareness:[14]

1. **Where is the evidence that the program will actually work?**
   Before such dangerous programs are implemented, policymakers need hard evidence – not speculation – that they will work.

[13] Loy, testimony, op. cit. The point cited here was made during the question-and-answer period.

[14] The Senate Commerce Committee is also asking questions about CAPPS II. On May 8 the Senate unanimously passed a provision requiring TSA to deliver a report on the program. See Audrey Hudson, "Hill assumes oversight role on airline screening," *Washington Times*, May 10, 2003.

2. **What will the error rate be?**
   Congress needs to know the likely false negative (incorrectly allowing a terrorist to pass) and false positive (incorrectly flagging an innocent person) rates for these systems, and what the estimates are based upon. Because the number of terrorists is so small in comparison to the overall population, false positives are especially likely to be a problem.

3. **How much will the program cost to build and operate?**
   The Congress was recently asked to provide $35 million to build CAPPS II.[15] (In a presentation given to us by TSA at Wye River, we were told it would cost just over $35 million to both build and operate the system). Given the enormous scope of this system – processing a billion records for 100 million separate passengers, correcting errors, fielding complaints, connecting computer systems to every airline counter in the nation – that figure strains credulity. What is the real cost, and what other security measures (for example, aircraft anti-missile systems) might we be giving up to pay for these programs?

4. **Is there a credible method for the falsely accused to get off the list?**
   The right to travel is a core human liberty. If some people are going to be deprived of that liberty – in effect, punished – they must have genuine due process. That must include real access to the records on which such decisions are made, and access to some kind of neutral magistrate who can evaluate the fairness of the deprivation of liberty. How will such due process be provided in a system based on secret government databases? Or will unfairly profiled passengers have to rely on the very same government agency that made the mistake in the first instance?

5. **What laws are in place that will protect us?**
   What current laws would protect against unauthorized abuses of our private information – and more importantly, the authorized misuse of our private data?

6. **What will be the cost to our privacy and freedoms of building these systems?**
   In light of the historical fact that government agencies and surveillance systems alike tend to expand and not contract, can we really restrict these kinds of programs to their original purpose?

Chaining the surveillance monster

TIA and CAPPS II are the ultimate expressions of a growing surveillance monster. If we do not take steps to control and regulate surveillance to bring it into conformity with our values, we will find ourselves being tracked, analyzed, profiled, and flagged in our daily lives to a degree we can scarcely imagine today. We will be forced into an impossible struggle to conform to the letter of every rule, law, and guideline, lest we create ammunition for enemies in the government or elsewhere. Our transgressions – whether real or imagined – will become permanent Scarlet Letters that follow us throughout our lives, visible to all.

---

[15] Loy, testimony before the Senate Appropriations Subcommittee on Homeland Security, May 13, 2003. Online at http://appropriations.senate.gov/releases/LoyMay13.pdf.

Some commentators have already pronounced privacy dead. The truth is that a surveillance society does loom over us, and privacy, while not yet dead, is on life support. It is not too late to put chains on the surveillance monster. The Congress acted properly by curtailing both the utility-worker informant program TIPS and TIA, and by requiring a review of CAPPS II. But you need to remain vigilant, and continue to resist programs that will make us neither safe nor free.

Total Information Compliance:
The TIA's Burden Under The Wyden Amendment

A Preemptive Analysis of the Government's Proposed Super Surveillance Program

Prepared by

American Civil Liberties Union
Technology and Liberty Program

Monday, May 19, 2003

Late last year, media reports began to surface on a secretive project underway at the Pentagon's main research wing, the Defense Advanced Research Projects Agency. The project, led by retired Admiral John Poindexter, a longstanding booster of high-tech intelligence gathering, carried the ominous moniker "Total Information Awareness."

As described in documents and statements by TIA officials, the program was an infrastructure for monitoring all transactions made by Americans in both government and corporate electronic databases around the world. It would be able to track every American's shopping habits, finances, travel plans, medical records, and many other activities – and then use complicated and questionable mathematical formulae to identify patterns that supposedly pointed to potential terrorist activity.

TIA became a magnet for criticism from across the political spectrum. Conservative talk radio hosts, concerned at the potential misuse of such a system by a left-leaning administration, joined with liberal pundits in demanding that TIA be abandoned. Others questioned the feasibility, practicality and cost of the system's stated mission. Conservative *New York Times* columnist William Safire called TIA an "super-snoop's dream."

In response to the widespread public outcry over TIA, members of Congress began to draft legislation that would put the brakes on the spy program. In January 2003, Congress passed a measure proposed by Sen. Ron Wyden (D-OR) that banned the use of TIA against Americans and prohibited further work on the program unless DARPA provided a report within 90 days containing:

- A "detailed explanation" of the program
- An assessment of the "likely efficacy" of TIA
- An assessment of the "likely impact" of TIA on "privacy and civil liberties"
- "A list of the laws and regulations that govern the information to be collected by" TIA

The government is expected to deliver its TIA report to Congress on or around May 20, and the first thing that Congress and the American people will need to evaluate is whether DARPA has adequately answered these questions.

There has been a great deal of confusion over the goals and mechanisms of the TIA program, much of it a result of seemingly contradictory statements issued by TIA officials themselves. But even after the most recent official description of the program, which was offered by DARPA Director Dr. Tony Tether in testimony before Congress on May 6, 2003, substantial questions remain.

This report was written by Jay Stanley, Communications Director of the Technology and Liberty Program of the ACLU.

What follows is an outline of the outstanding questions and issues we believe the report must address and answer in order to comply with Congress's directive.

1. A detailed explanation of the actual and intended use of funds

Before Americans can weigh the costs and benefits of the TIA program, they need clear answers about exactly what the program's limits and potentials are. Some confusion over TIA's capabilities stems from the fact that DARPA (as the agency constantly points out) is creating a tool, the use of which will fall to another agency or agencies. That means that DARPA cannot itself answer the question of how the system will be used. Rather, questions must be asked in terms of what the system is *capable* of doing.

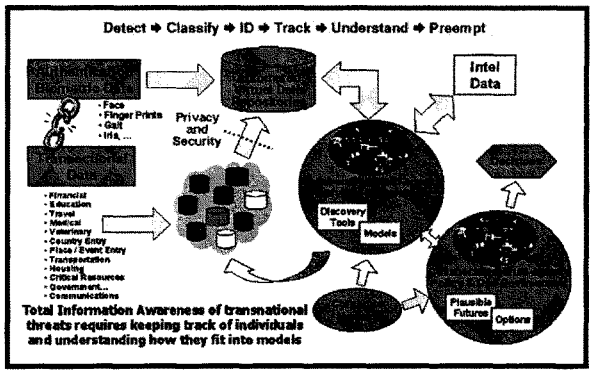
TIA's developers must supply definitive answers to the following questions about its operation:

A. Would the system be capable of connecting to and searching through an arbitrary number of distributed databases?
Will the number or composition of the databases accessed with TIA be in any way limited or hard-wired, or will the government agencies using the system have complete freedom to search as many databases of as many different types as they can legally access?

From a civil liberties perspective, this is a crucial question. If TIA can easily be scaled up to draw in more and more sources of data, then the technological path is clear for the program to turn into the all-encompassing surveillance tool that DARPA has denied it would become.

In his testimony, Dr. Tether denied that TIA planned to "use transaction data held by private companies." "I don't think we've ever said that," he said.[1] However, DARPA's own materials contain an extensive list of the categories of information planned for inclusion in the system (see chart). In addition, at the very same hearing where Dr. Tether spoke, a representative of the FBI admitted that "the FBI does utilize public source data." Given that it will be the FBI and other agencies and not DARPA that will actually deploy TIA, it is crucial that Congress be told what the system will be *capable* of searching, not just what DARPA with its ever-changing explanations now says.

[1] Testimony of Dr. Tony Tether before the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, May 6, 2003. The comment quoted here was made during the question-and-answer portion of his testimony.



B. Would the system be capable of being used with a centralized database?
TIA officials have recently stressed that the system would be designed to work with scattered or distributed databases tied together, not a single centralized data repository. That seems to contradict earlier descriptions of the program, such as a chart describing the operation of the program that prominently features "automated virtual data repositories." That chart was featured on the TIA Web site and taken down after a firestorm of public outrage over the program erupted.

Of course, even if DARPA staff does not design TIA with a centralized database in mind, there is no reason why, once the product is finalized, that FBI agents or others elsewhere in government could not attempt to do so. Presumably, if the system can search through multiple databases, it should have no problem searching through a single database. Would TIA be *capable* of doing so, even if that is not how it is originally designed to be used?

C. What kinds of information analysis would the system be capable of?
Would TIA have the capacity to perform any kind of search for correlations or other statistical analysis, or other commonly used data-mining techniques (such as Exploratory Data Analysis, neural networks, etc.)? If not, could those capabilities, which involve highly intrusive searches through individuals' lives, be attached to the system at a later time?

In comments and documents made before the eruption of public outcry over TIA, program officials often seemed to suggest that this kind of data mining was what they had in mind. Admiral Poindexter, the head of TIA (and the most senior official implicated in the Reagan Administration's Iran-Contra scandal), told an audience in August 2002, for example, that "one of the significant new data sources that needs to be *mined* to *discover*

and track terrorists is the transaction space."[2] Another top TIA official, Ted Senator, told the same audience that TIA was "all about" connecting information into "patterns that can be evaluated and analyzed, and learning what patterns discriminate between legitimate and suspicious behavior."[3]

One observer in a position to know what is going on in government is Gilman Louie, the head of In-Q-Tel, a venture capital fund established by the CIA. He says that the merits of data mining are the subject of "an ongoing argument" and "a big debate right now in government."[4]

DARPA says that it has been misunderstood. In his congressional testimony, Tether said that TIA will not involve sifting through everyone's information looking for models of what terrorist behavior might look like:

> When most people talk about "data mining," they are referring to the use of clever statistical techniques to comb through large amounts of data to discover previously unknown, but useful patterns for building predictive models. . . . DARPA is *not* pursuing these techniques.[5]

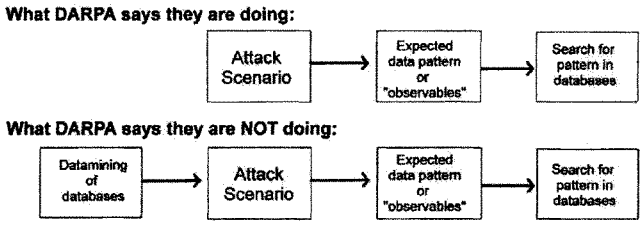
The TIA's actual approach, Tether, said, would be different:

> Our approach starts with developing attack scenarios. . . . These scenarios would be based on expert knowledge from previous terrorist attacks, intelligence analysis, new information about terrorist techniques, and/or from wargames in which clever people imagine ways to attack. . . .

The process he describes is one of query-based searches rather than data mining. "We create models, and say 'these would be the observables'" or behaviors that would be expected to flow from those models, the DARPA chief said. "We then take that pattern to the databases, and see if that pattern exists."[6]

---

[2] Admiral John Poindexter, speaking at a DARPA conference in Anaheim, California, August 2, 2002. A copy of Poindexter's prepared remarks is online at http://www.fas.org/irp/agency/dod/poindexter.html.
[3] Senator is head of the "Evidence Extraction and Link Discovery Program" (EELD), a part of TIA. His comments are posted online at http://www.darpa.mil/DARPATech2002/presentation.html.
[4] Steve Lohr, "Data Expert is Cautious About Misuse of Information," *New York Times*, March 25, 2003.
[5] Written statement of Dr. Tony Tether submitted to the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, May 6, 2003, pp. 1-2. Emphasis in original.
[6] Tether testimony, May 6, 2003. The comment quoted here was made during the question-and-answer portion of his testimony.



Under both methods, the users of the TIA system would generate theories about what terrorists might be planning ("attack scenarios") and then search through databases looking for evidence of those theories. But when it comes to the question of how those attack scenarios will be generated, DARPA denies that it will be by an initial search through the databases for "suspicious patterns." Rather, they would be generated through intelligence analysis, "expert knowledge," and wargames in which clever people "imagine" possible attacks.

Whether TIA officials have changed the program's goals, have just put a new gloss on what they intend to do, or have been genuinely misunderstood from the beginning, is far from clear. But even if we accept DARPA's current, more modest description of what they are building, the program still appears to pose an enormous threat to Americans' privacy, and there are important questions about its operation that must be answered.

First, it is important to understand exactly how analysis of the TIA database will be conducted under real-world conditions. In truth, few data mining techniques involve trying to approach a set of numbers with no theories or models to test; there is always a complex interplay between theories and data. As creative and experimental analysts repeatedly ran, modified, and re-ran their attack scenarios through the TIA system, it would not be surprising if many of their searches began to resemble or duplicate the techniques used in data mining. Curious and aggressive agents will inevitably push the system to its hard-wired limits; it is important for Congress to be told what those limits will be.

Finally, the recognition by DARPA officials that a statistical analysis or data-mining strategy is (in Tether's words) "ill-suited to ferreting out terrorist plans" does not mean that it could not be tried at a later date by agents at the FBI or another agency that uses TIA, who might not possess the same understanding of the limits of data-mining. That is why it is important to establish the *capabilities* of the TIA system.

In the end, it is important to remember that every version of TIA that has been described, including pattern recognition, involves searching through billions of records about hundreds of millions of Americans.

2. The likely impact of TIA on privacy and civil liberties

By creating the means of combining together information on Americans' personal lives from many different sources into one rich view of their lives, the TIA program will bring into existence an immensely powerful surveillance tool. Like the atomic bomb, that tool will change the world just by being brought into existence, because it is so powerful that even if it is not used (or not used fully), the mere prospect of such use will change everyone's behavior. Given that reality, there are numerous questions that must be answered in fulfilling Congress's request for an assessment of the program's impact on privacy and civil liberties.

A. What difference would a distributed database make?
TIA officials have recently been touting the fact that the system would be based on distributed databases, and not one large central compendium of information, as a reason not to worry about the program. In today's world that is a distinction without a difference. Communications technologies like the Internet now make it possible to build a system for searching multiple databases all over the world that is, from the user's perspective, completely indistinguishable from searching a single, local, centralized database. (Millions of people experience that phenomenon every day when they use Internet search engines like Google.) Admiral Poindexter was referring to this fact when he declared that TIA's goal is to "develop ways of treating the world-wide, distributed, legacy databases as if they were one centralized database."[7]

The difference between centralized and distributed databases is invisible to the user, and makes no difference for privacy. No matter what the database architecture, the important thing is what information is available to the users. If anything, a distributed architecture appears to make possible far more powerful and up-to-date database than would a centralized repository. TIA needs to answer the question of how a distributed database would benefit privacy and civil liberties, or acknowledge that the distinction is irrelevant.

B. How can Americans be free when their every move is open to potential scrutiny?
As many a suspicious employer knows, individuals are just as affected by the knowledge that we *might be* under observation as we are by the *certainty* that we're being watched. When you don't know whether or not you're being monitored, the safe thing to do is to act as if you are at all times. Even under the more restrictive, query-based version of TIA, it will always be possible that our innocent activities will coincide with the latest imaginative "threat scenario" being explored at TIA Central, placing us under a microscope.

When every recorded activity in which Americans participate becomes subject to potential review by federal agents, American life, always distinguished by its open, free-wheeling nature, will fall under a cloud. Clearly, Americans don't want everything they do watched by the government. DARPA needs to address the issue of how TIA can be

[7] Poindexter, Anaheim, Calif., August 2, 2002.

implemented without violating that principle given the fact that potential monitoring is just as potent a source of control as actual monitoring.

C. What are the limits of privacy-enhancing technologies?

Imagine that the government set up computers that recorded every telephone call made in the country, converted the audio signals to text, and analyzed their contents without disclosing them to any human beings. The computer then alerted the authorities to any conversations that matched descriptions of "threat scenarios" entered by government security agents. Or, imagine that the government installed video cameras throughout every home in the country, and fed the video images to a computer, which analyzed the images and recorded descriptions of the behavior it observed, again without disclosing anything to the authorities.

Even if the authorities had to get a warrant in this scenario to access our information and discover our identity (and most of the data TIA would search could be obtained without one), all the bad effects that come from government spying would be felt: feelings of being monitored, a restricted sense of freedom, a chilling of free speech (especially speech critical of the government), and potential abuses of power. Even if the records of our every move and our every conversation were "anonymized" by special privacy-protecting technologies but could still be perused by agents testing their latest imaginative threat scenario, we would no longer be free. In effect, a government informant would be listening to every call and watching our every move, constantly prepared to call us to the attention of the authorities. The fact that that informant is a computer would be of little comfort (and might even be worse).

TIA, in essence, is a proposal to set up a system to do just this. Although it would spy on our transactions rather than our conversations and our behavior in the home, the information assembled by TIA would offer a view into our lives that would be scarcely less intrusive – especially as the cloud of transactional information captured about each of us continues to thicken. And the simple fact is that there are no real legal impediments to the government gaining access, through purchase and cooperative disclosure, to virtually all of the "transaction space."

Although our imaginary video and telephone-monitoring system would not be possible under current interpretations of the Constitution, the American legal system has not yet had a chance to extend those interpretations to cover the transactional information that would be assembled by a TIA system. The builders of TIA propose to exploit this growing gap in our privacy protections and build permanent institutions around it.

D. How can the bedrock Anglo-American principle of "individualized suspicion" be maintained?

It has always been a core principle of the American legal tradition that the government is not allowed to spy on you unless it has *individualized suspicion* that you are involved in wrongdoing. The government is not allowed to spy on you as part of a broad fishing

expedition, or because you are a prominent (or not-so-prominent) member of the Republican party, the Democratic party, the ACLU, or the Eagle Forum. DARPA needs to explain how the principle of individualized suspicion can be squared with a system that:

- **Exposes every American to the possibility of having all their transactions scrutinized by the government.** That exposure would take place on no basis other than the fact that a person's activities happen to coincide with a speculative scenario for possible terrorist activity dreamed up by a government security agent.
- **Effectively asks every American a specific question about their life every time the system is searched.** For example, if a security agent were to come up with a model that includes people who have recently purchased several garden hoses, the TIA system would then have to search its database for people who fit that description. It would do so by examining *every person* in the database, and looking to see whether they have recently purchased garden hoses. That means that every time a query is run, a person is, in effect, being asked a question about their life by the government. Except that that query takes place in secret; looks at data that an individual might not even be aware has been collected about them; and leaves the individual no leeway in how the question is answered and no chance to explain away the presence of any flukes, errors, or unusual circumstances.

E. How will TIA likely affect privacy and civil liberties over time?
DARPA's assessment of the civil liberties implications of TIA must examine not just how TIA is likely to operate the day after it is turned on, but how it is likely to evolve over time given certain well-observed tendencies that are found in governments and in human beings across time. Its analysis must be diachronic (concerned with how something changes through time) rather than synchronic (concerned with how something appears frozen at one moment in time).

In particular, what are the likely implications of TIA in light of certain time-tested historical realities:

- The tendency for government agencies to expand and not contract in size and power. As TIA grows, will it form a powerful bureaucratic lobby for increased surveillance in American life?
- The tendency of information systems to grow, not only in the data they collect, but in the uses to which they are put. Once the system is in place, will its operators grow frustrated at the gaps in its coverage, and seek to have more and more transaction records available to them? Will TIA be expanded from terrorists to murderers to thieves, and so on down the scale of wrongdoing until everyone is put on guard against the slightest infraction of every law, rule, regulation, and social code in America? Since no wrongdoing, however small, is truly defensible, at what point will the nation draw the line?
- The tendency for law-enforcement and other government agencies to find their mission twisted from time to time by their political overseers toward political ends.
- The occasional emergence of periods in American history of intense social and political conflict, such as the Vietnam anti-war and Civil Rights movements and the

labor movement earlier in the century – and the intense fear of terrorism that we are now experiencing.
- The tendency of law enforcement agencies and personnel to take sides in those conflicts.

Even if we accept the premise that it would be possible to build a perfect system that allowed government agents to browse through records of individuals' activities under a regime of unimpeachably watertight privacy protections (although neither the technology nor the privacy laws for such a regime now exist), how long would such a system be likely to remain watertight under the immense pressures to which it will be subjected over time?

Build a system for perfect surveillance and they will come.

The American founding fathers took a long-range perspective when they set up our democracy. Even though everyone knew that perhaps the most trusted man in the nation – George Washington – was going to be president, the founders still set up a system of government based on checks and balances. They knew that temptations and attempts to abuse power were, over time, inevitable – and because the Constitution they drew up incorporated that recognition, the United States has been for 200 years the world's most stable democracy.

Our Constitution was built to last, and policymakers today contemplating surveillance systems with a potentially revolutionary impact on American life have a responsibility not to cast aside that wisdom and install the seeds of an institution that will corrode our freedom, either suddenly or over time.

3. The likely efficacy of TIA

Serious questions have been asked about the likely efficacy of TIA. Given the substantial civil liberties implications of TIA, DARPA must meet a very high standard in demonstrating its likely effectiveness in catching terrorists and saving lives.

Gilman Louie, the head of In-Q-Tel, said in March that he thought that the data mining approach is too blunt an instrument to be a primary tool of surveillance. "I think it's very dangerous to give the government total access," he said.[8] The Association for Computing Machinery has also expressed serious doubts about the program's feasibility:

> The overall surveillance goals of TIA suffer from fundamental flaws that are based in exceedingly complex and intractable issues of human nature, economics and law. . . . As computer scientists and engineers we have significant doubts that

[8] Steve Lohr, "Data Expert is Cautious About Misuse of Information," *New York Times*, March 25, 2003.

the computer-based TIA Program will achieve its stated goal of "countering terrorism through prevention."[9]

DARPA has always traditionally tackled research tasks that are extremely difficult and futuristic in nature – an often-celebrated quality that has even led to projects of uncertain feasibility being called "DARPA-hard." While such boldness may be admirable in many cases (such as language translation), the calculus is different when it comes to projects with enormous social and political implications. In the case of TIA, where the intrusion on privacy is virtually certain, the slim chance of success places a heavy burden on DARPA to demonstrate the benefits of its project. After all, it is entirely possible that TIA would lead to dangerous invasions of privacy while still failing as a means of stopping terrorism. At the very least, DARPA must address several key questions that have been raised by observers about the feasibility of the TIA concept:

How bad will the problem of false positives be?
Given that there are approximately 300 million residents of the United States, and in all probability no more than a handful of persons planning terrorist attacks, the question of how many people will be falsely flagged or accused of being a potential terrorist by a system like TIA is a vital one.

The consequences of being falsely singled out as a potential terrorist can range from having one's privacy invaded, to enduring inconvenient and humiliating security checks, to damage to career or reputation, harmful notations in one's record, to arrest and imprisonment. Already since the 9/11 terrorist attacks, we have witnessed the damage that such accusations can do. Many immigrants were unfairly imprisoned, often for months at a time. The FBI under its "Project Lookout" gave corporations a list of hundreds of names of people it sought in connection with September 11. The list, which was riddled with inaccuracies and contained the names of many people the Bureau simply wanted to talk to, was widely circulated and took on a life of its own. No one knows how many innocent people have been denied jobs or suffered other harm because of the list.[10] And the government's "no-fly" list of terrorist suspects has been a similar disaster, ensnaring hundreds of innocent Americans who find themselves facing intense security scrutiny every time they fly, with no way of finding out how they got on a list or how to get off.[11]

As a little simple math shows, even a system that is 99% accurate will generate disabling numbers of false positives under a data mining system. The population of the US is about 300 million. If we assume that there are an additional 1,000 terrorists living here, a 99% accurate system would catch 990 of them. But it would also flag 3 million innocent

---

[9] Association for Computing Machinery Public Policy Committee, letter to Sens. John Warner and Carl Levin, January 23, 2003. Available online at http://www.acm.org/usacm/Letters/tia_final.html.
[10] WSJ – get cite - article on or about Nov. 19 '02. Ann Davis, "Far Afield: FBI's Post-Sept. 11 'Watch List' Mutates, Acquires Life of Its Own," *Wall Street Journal*, Nov. 19, 2002.
[11] An ACLU press release on the case is online at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12439&c=206. In addition, the Electronic Privacy Information Center has posted hundreds of complaints filed by passengers at http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html.

Americans as terrorists. That would leave a total of 3,000,990 people who have been identified as terrorists – and of course the authorities won't know which among them are the real terrorists.[12] The amount of investigative effort that would be involved in winnowing that field would be staggering. More realistic assumptions show even more dysfunctional ratios of real catches to false alarms.

Number of non-terrorists living in US	300,000,000	300,000,000	300,000,000
Number of terrorists living in US	1,000	1,000	1,000
Accuracy in identifying terrorists as terrorists	99.99%	99.00%	50.00%
Accuracy at identifying innocent as innocent	99.99%	99.00%	97.00%
# of terrorists who will be caught	1,000	990	500
# of innocent people who will be "caught"	30,000	3,000,000	9,000,000
Total # of people flagged as "terrorists"	**31,000**	**3,000,990**	**9,000,500**
Of those, number who really are	**1,000**	**990**	**500**

In short, this kind of a system rapidly becomes useless unless extremely high levels of accuracy can be maintained – levels that are, in fact, completely unrealistic.

We are told that the problem of false positives would be less severe on a system that is based on scenarios generated by analysts rather than scenarios generated through statistical analysis or data mining. But that assumes that the scenarios are themselves going to be accurate. Given the creativity of both terrorists and the analysts trying to anticipate their attacks, the number of "threat scenarios" that could be imagined is nearly infinite. In addition, many attacks could be imagined that involve transactions that are extremely common and match the activities of hundreds of thousands or even millions of people.

How much behavior would the system have to monitor to be effective?
Even if it is installed to the maximum extent, the TIA system would only be able to search and analyze those activities that leave behind electronic records. Electronic transactions that are not stored in databases, cash or paper transactions, and illegal or black-market activities would not leave traces in the searchable "transaction space" and so would not be covered by any queries launched by TIA operators.

Ironically, activities that leave no or fewer trails are precisely the sort of transactions that real terrorists, who strive to live "below the radar," will engage in. TIA could easily be the kind of system that sweeps up the innocent rather than the guilty.

[12] This problem has been pointed out by several experts, including computer scientist Benjamin Kuipers of the University of Texas at Austin, analysis online at http://www.interesting-people.org/archives/interesting-people/200212/msg00061.html and Bruce Schneier, http://www.counterpane.com/crypto-gram-0304.html.

That point is crucial because unfortunately what is likely to happen is that the information available to the TIA's computers, while representing an enormous amount of data about Americans' personal lives, will not be enough to fully explore the threat scenarios dreamed up by security agents. The result will be that the institutions that operate the TIA system will work to envelop more and more sources of information into the system, and push public officials to expand the kinds of information that they can legally include.

4. The laws and regulations that govern TIA

Congress has asked DARPA to survey the existing laws and regulations that would govern the TIA program. That is an important exercise, but it is largely irrelevant to the larger policy questions raised by the TIA program. That is because current privacy laws largely don't cover government access to the kind of third-party transactional information – financial, medical, education, travel, transportation, housing, communications – that TIA envisions using.

Medical information, for example, is subject to a complex new set of privacy regulations, but those regulations (known by the acronym HIPAA) permit broad access by law enforcement to patients' records. In another example, the FBI reportedly has an $8 million contract allows government agents to tap into the data aggregator Choicepoint's vast database of personal information on individuals.[13] Although the Privacy Act of 1974 banned the government from maintaining information on citizens who are not the targets of investigations, the FBI can now evade that requirement by simply purchasing information that has been collected by the private sector.

TIA officials are fond of emphasizing that their program "will comply with all the current privacy laws." But the reason that TIA is such a fiercely debated topic is precisely that the laws in this area have been totally outstripped by technology. The law didn't anticipate several factors that have emerged in recent years:

1. **The growing collection of information in private databases.** With the use of computer chips in everything from car and office keys to cell phones to transit passes, and with the private sector's discovery that it is very profitable to gather, analyze, and sell information on customers, more and more information is being collected about more and more of our activities.
2. **The ability to conduct mass sweeps through data.** Until recently our privacy has been protected by the fact that it was difficult or impossible to bring together information about individuals collected by different parties at different times and places. Searching for information across different databases used to be a cumbersome, time-consuming process. But today the Internet allows for the instantaneous sharing of databases that once would have had to be copied onto tape reels and physically shipped. And the increasing standardization of data

[13] Glenn R. Simpson, "Big Brother-in-Law: If the FBI Hopes to Get The Goods on You, It May Ask ChoicePoint" Wall St. Journal, April 13, 2001.

formats as well as advances in database-merging technology makes information increasingly easier to compare.

3. **The emergence of distributed databases.** As discussed above, the distinction that has been built into our privacy laws between information that the government itself "maintains" and information held by others that is open for the government to *access*, is now obsolete.

A delicate and careful balance has been constructed in American life between individuals' right to privacy and the government's right, in some situations, to spy on people. Initially set by the Constitution's Fourth Amendment, that balance has been readjusted over the years in response to new technologies ranging from the telephone to thermal imaging devices. Often, it took the courts many years to adjust to new technologies – telephone conversations, for example, were not folded under the Fourth Amendment for several decades.

One can hope that eventually our legal system will extend privacy protections to fill in the gaps created by these developments. But the Total Information Awareness program and the technologies behind it – new ways of collecting, storing, and assimilating information about Americans' daily activities – would rush into the current gap created by the law's lag behind technology, and create powerful institutions with a vested interest in maintaining and expanding that gap. The simple fact is that the technology is developing at the speed of light, while the law crawls along at a tortoise's pace. TIA or its equivalent could be the perfect storm of surveillance from which we have no shelter.

Mr. PUTNAM. Thank you.

Can we pass those charts up here so the subcommittee members can actually see them?

I will note for the record the arrival of the gentleman from Ohio, Mr. Turner. We welcome him to the subcommittee and the record will be open for your opening statement in the appropriate spot.

Our final witness today is John Cohen, co-founder, president and CEO of PSCom LLC, Inc. He oversees the general corporate operations as well as the strategic development of the firm. Mr. Cohen is also director of the Progressive Policy Institute's Community Crimefighting Project and co-director of the PPI Homeland Security Task Force. He has served as a policy advisor to a number of local, State and national administrations and political campaigns including as coordinator of the State of Maryland's Public Safety Technology Task Force and special advisor to the Governor's Cabinet Council on Crime and Juvenile Justice.

Mr. Cohen has written and lectured extensively on many issues advocating the deployment of existing and new technologies in business practices to fundamentally change the way we provide for the public safety in America. These issues include homeland security, counter terrorism, community policing, drug policy, public safety and racial profiling by police.

Welcome. You are recognized.

Mr. COHEN. Thank you for the opportunity to participate in this important hearing.

My views on this issue come from the perspective of someone who has spent the last 20 years in law enforcement, both from the operational oversight and policy development perspective. I have worked counter terrorism cases as a special agent for the Office of Naval Intelligence and worked as a police officer assigned to Federal agencies. I appreciate the opportunity to be a part of this discussion.

As we look back at what has happened in this country since September 11, I think the best way to describe how State and local governments have responded and have been operating has been purely in a reactive mode. It has been a reactive mode based on non-specific and vague information that has been provided. This shouldn't be a surprise to everybody because prior to September 11 the information sharing amongst our Federal, State and local law enforcement agencies was ad hoc at best, based on personal relationships very often and not supported by an integrated system of law enforcement information sharing.

While this homeland security approach may have been appropriate for the months immediately preceding the events of September 11, Governors and mayors around the country have come to the conclusion that from a long term perspective, they can no longer operate in a manner in which with every threat level elevation, they are going to take police officers out of their communities and mobilize the National Guard to have them guard potential targets.

There is a growing consensus that our Nation's homeland security issues should be driven by a number of basic principles. First, the front lines of the Nation's war on domestic terrorism are our cities, towns and local communities. Therefore, State and local authorities must be active partners with the Federal Government and

develop strategic and operational plans related to homeland defense.

Second, the loss of life and financial repercussions that would result from a successful terrorist incident require that State and local governments take a preventative approach, not just be prepared to respond. In this regard, State and local homeland security efforts must be information driven, proactive and focused on preventing future attacks. This can best be done by collecting, analyzing and disseminating critical information, not just giving it to the Joint Terrorism Task Forces but putting systems into place so that information obtained by a beat cop in a community can flow up and be part of the analytical mix as well as critical information flowing down to that same beat cop.

This debate, while important, must be done in the context of the following. Almost 21 months after the attacks of September 11, this Nation still has not taken critical steps in creating a strong information sharing capability that allows us to conduct this collection, analysis and dissemination of vital information. We knew connecting the dots was a problem prior to September 11 and to be quite frank, it is still a problem now. I have spent the last 21 months working with a number of city and State governments helping them look at the issue of homeland security and develop plans on how they can be better prepared to stop future acts of terrorism. Overwhelmingly what I hear from mayors, Governors, police chiefs, fire chiefs and public health officials is that we aren't putting the emphasis into prevention that we should. A critical part of those prevention efforts is linking these information systems.

While it would be great to have systems like TIA and be able to go into credit histories of people that potentially may be terrorists, it would be great to have a new radar system that allows us to identify through gait individuals. While there are amazing things we can do with biometrics and facial recognition, the fact of the matter is none of those systems will work if we don't create an initial foundation of criminal justice information sharing that allows us to share basic police information.

Many of you from this area were here last summer during the sniper incident—3 weeks which paralyzed this region. What is incredible about that whole situation is the car that contained both suspects in that case was stopped over 10 times by law enforcement authorities, entered into law enforcement systems and never rose to anyone's attention. When phone calls were being received in the call center during the sniper incident, the information was put on pieces of paper, stacked in piles behind the calltakers and at some point during the day, it was disseminated to local agencies so those leads could be followed up.

This is not an information sharing system that is going to help us stop the next act of terrorism. As we begin the process of investing billions of dollars in homeland security, beefing up this capability has to be a top priority.

Let me conclude that as we look at expanding the information sharing capability, oversight is a critically important part of that. September 11, unfortunately, did not stop the fact that some in law enforcement abuse authority, and while most cops are honorable people, we have to make sure oversight mechanisms are in place

to prevent abuses of information collection capability and punish those who misuse it.

Thank you. I will respect the time rule also since everyone else did.

[The prepared statement of Mr. Cohen follows:]

Testimony of John D. Cohen
President & CEO, PSComm, LLC
Before the House Government Reform Committee's
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
May 20, 2003

Can the Use of Factual Data Analysis
Strengthen National Security? - Part Two

Introduction

Good morning Chairman Putnam, Vice Chairwoman Miller, Ranking Member Clay and other distinguished members of the subcommittee. Thank you for this opportunity to participate in this critically important hearing.

The comments and observations I offer today are based on having spent my entire career – close to 20 years – involved in law enforcement operations, oversight and policy development. My views on this issue come from a somewhat unique experience base that includes service as a:

- Special Agent in the Office of Naval Intelligence;
- Police officer who regularly worked side by side with federal agents to conduct investigations of international criminal organizations;
- Senior investigator for a Congressional committee that conducted oversight reviews of our nation's intelligence and law enforcement efforts;
- Policy advisor to the Director of the Office of National Drug Control Policy; and
- A homeland security advisor who has helped a number of city and state governments assess and improve their ability to detect, prevent and respond to acts of terrorism.

First, let me clearly state that if we as a nation are truly serious about preventing acts of terrorism, we have to dramatically improve the flow of information among federal, state and local law enforcement entities. We also need to enhance our ability to provide front line law enforcement personnel (whether they are investigators assigned to a joint terrorism task force or beat cops) with accurate, timely and useable information. This was an issue prior to the attacks of 9/11 and as we all know, our inability to "connect the dots" was identified during the post-attack inquiries as a significant problem.

It is now almost 20 months after the attacks of 9/11. Yet despite universal recognition of the problem, we have not taken the necessary steps to establish a national law enforcement information sharing capability that facilitates the collection, analysis and dissemination of law enforcement information so that we can "connect the dots." This represents the most serious impediment to our nation's efforts to prevent violent crime and stop future acts of terrorism.

Data mining or factual data analysis can serve a critical role in strengthening both day-to-day crime prevention and homeland security. We need to clearly define what type of information would be most valuable in accomplishing that goal and what type of systems would best support our efforts to stop future terrorist attacks. And we need to do this now, as we begin investing finite tax dollars into researching, developing and implementing complex, new electronic monitoring and detection tools that allow law enforcement to discover the activities of potential terrorists. That is why Mr. Chairman, I congratulate both you and this Committee for holding hearings on an issue that I believe is at the heart of our nation's ability to protect the public.

Where are we today?

After almost 20 months since the attacks on the World Trade Center and the Pentagon, the view from government officials who serve at the front lines of our domestic war on terrorism is that very little has changed from the perspective of information sharing. In some ways things have gotten worse.

Prior to the events of 9/11, information sharing among law enforcement agencies was based on personal relationships. When I was a police officer, we used to have a saying: "Cops share information; agencies don't." What this means is that if a police officer from one agency happens to have a good relationship with a cop from another (or even a local FBI agent), then there is a mechanism for the sharing of information about investigations and other relevant issues. Absent that type of relationship, information sharing was often more difficult. But even when the sharing of information did occur, it involved phone conversations, faxes or traveling to meetings to exchange paper documents. Because there was no infrastructure to support the sharing of key investigative type information, it was often left to individual law enforcement personnel to establish the mechanisms and, in some cases, the information systems that facilitated the exchange of information. In the late 1980s and early 1990s, the emphasis was placed on establishing pointer index-type systems so that if one police officer had a name or an address of interest, he or she could be directed to an investigator in another agency who may have additional valuable information.

Recognizing that information sharing through phone calls, meetings and faxes was not truly an effective way to facilitate data mining, information analysis and therefore the solving and prevention of crime, the late 1990s saw growing interest in the establishment of "integrated justice" systems. These systems linked federal, state and local criminal justice information, so that information could be shared electronically and proactively. At the same time, police agencies began to focus on moving away from the reactive strategies that drove police operations. They started to become more information driven and proactive. Many police agencies set a goal to enhance their ability to prevent crime by analyzing crime and other related data, identifying emerging crime problems and implementing operational strategies designed to prevent situations from escalating into emergencies. Thus began the process known as COMPSTAT.

Post 9/11, the sharing of information between law enforcement has at best remained the same but in some respects has become more difficult.

Arguably, there is greater recognition throughout the law enforcement community that information sharing is important. And in those jurisdictions in which strong interpersonal relationships exist, information sharing continues to be positive. But in those areas of the country where interpersonal relationships do not exist, information sharing is not as effective. The result is ad-hoc and inconsistent information sharing and cooperation among law enforcement entities.

More importantly, despite a tremendous amount of rhetoric, there has been little to no progress in establishing a truly integrated law enforcement information system that facilitates the flow and analysis of information among the nation's law enforcement agencies.

- Many police, public health entities, parole officers and courts are operating with 20-year-old information technology.
- Even though high-speed digital technology is currently available, many police officers still wait long periods to receive basic information about a vehicle or person they stop.
- In some states, days or weeks may pass before criminal warrants find their way into state databases, leaving dangerous criminals on the street and police without this information.
- In many states, judges might sentence offenders with outdated information regarding their criminal history records.
- In most states, investigators in one jurisdiction may be unaware that information regarding an individual under investigation exists in a neighboring jurisdiction.

- The General Accounting Office reports that the 12 terrorist related watch lists maintained by various federal agencies are still maintained in stove-piped or non-linked information systems.
- Brian David Mitchell, the suspect in the Elizabeth Smart kidnapping case, spent six days in a San Diego jail, but was released because Utah authorities had not notified other law enforcement agencies that he was a suspect. And, it wasn't until a month later after the suspect was arrested, that authorities matched his fingerprints.
- During the three weeks when two snipers terrorized the Washington, D.C. area, various local police agencies stopped the vehicle containing both suspects on 10 separate occasions. Even though police ran the license plates through the national database, there was no record that the car had been stolen or its occupants were wanted for any crime.
- Even worse, weeks before the first sniper attack, a latent fingerprint of one of the alleged snipers was retrieved at the scene of a robbery homicide in Montgomery, Alabama. State officials in Alabama were unable to make the connection, because they were unaware that the fingerprint was on file with the federal government. Alabama only maintains a statewide crime database; it is not linked to the system that maintains federal information. Authorities only learned the truth when one of the sniper suspects told police about the robbery in Alabama, and a paper copy of the latent print was transported to Washington, D.C. and entered into the federal system. If the identification had occurred in a timelier manner, a felony warrant would have been place into the National Crime Information System (NCIC). Then, Montgomery County, Maryland police, who stopped a vehicle containing both suspects four hours prior to the first sniper shooting, could have made arrests. The sniper attacks would never have occurred.
- While the sniper attacks were ongoing, information received through a tip line had to be hand written on slips of paper and sent by fax or retrieved, because no electronic information system existed.

The fact that the information systems used by individual law enforcement agencies are not inter-linked directly impedes our ability to prevent future terrorist attacks. It is hard to believe that greater emphasis has not been placed on establishing "integrated justice" systems at a time when billions of dollars are being provided to federal, state and local governments in the name of homeland security. Perhaps the reason why is because for the most part, the federal government considers the role of state and local governments as that of "first

responders," ignoring the fact that state and local law enforcement play critical roles in detecting and preventing acts of terrorism.

Additionally, the Department of Justice has established an artificial separation between counter-terrorism and crime prevention efforts. Domestic terrorism is viewed as more of an intelligence issue, requiring separate processes and protocols than day-to-day crime fighting efforts.

The philosophy that somehow counter-terrorism is a domestic intelligence issue; crime is a law enforcement issue and both need to be treated separately is not only inefficient but also dangerous.

The first indication that a terrorist cell is operating within the United States may not come from information uncovered as part of an intelligence operation, but instead it may come from behavior discovered during an investigation by state or local police, looking into suspicious activity. We know that terrorists often use traditional crimes such as drug and illegal weapons trafficking, money laundering and bank robbery to offset costs and further support their political/terrorist objectives. Therefore, rapidly collecting and disseminating solid information about the people who commit crimes and the places where crime is committed is essential to our homeland security efforts.

Additionally, terrorists are dangerous, not because they say or believe dangerous things, but because their beliefs motivate them to commit acts of violence targeting people, places and things. These acts of violence – whether motivated by political or religious ideology – are still criminal acts. Is a mass murder that is motivated by political ideology any more sinister than a mass murder motivated by greed or mental illness? Preventing any act of violence within the United States should be a top priority, regardless of whether motivated by greed, criminal intent or ideology. Even prior to passage of the USA Patriot Act, mechanisms were in place to facilitate the sharing and use of sensitive intelligence information by domestic law enforcement agencies. These procedures and rules ensured that sources and methods were protected, while at the same time, dangerous criminals could be identified, investigated and prosecuted in a manner that respected the fundamental constitutional protections of all Americans.

Where do we go from here?

The loss of life and financial repercussions that would result from a successful terrorist incident requires that state and local governments do whatever they can to prevent such an attack from occurring. In this regard, state and local homeland security efforts must become information driven, proactive and focused on preventing future attacks.

These preventative efforts can supported by:

- Providing training to state, local and tribal law enforcement, public health and other government personnel, so that they are better able to identify signs that a terrorist group is operating within their midst; and

- Collecting, analyzing, and disseminating critical information so that beat cops, detectives, state troopers and other law enforcement personnel – regardless of their assignment – are better able to identify terrorist group operations.

A key component of any effort to protect the public from international terrorists or homegrown criminals is the rapid access by law enforcement and other appropriate personnel to information contained in local, state and federal databases. Currently 38 states and the District of Columbia have begun efforts to create "integrated justice" information systems, linking police, courts, corrections and other criminal justice components. These systems will allow for the rapid flow of information about the people who commit crimes and the places where crime occurs. Law enforcement officials and policy makers will be able to identify suspicious and unusual trends and develop information-driven strategies that effectively target criminals and the conditions that facilitate criminal activity. These same systems are essential components of any organized effort to prevent or respond to future critical incidents and terrorist threats. They also form the backbone for daily operations.

Accordingly, before the country invests millions of dollars creating a system that allows the government to track credit card information of innocent Americans, we need to make it a priority (and homeland security funding should be available) for each state to link the independent information systems used by city, county and state criminal justice entities to allow for the rapid flow of information about the people who commit crimes and the places where crime occurs. These statewide systems should then be linked to federal systems. This information sharing will support efforts by law enforcement to identify suspicious trends and effectively target those involved in criminal activity.

But, it is not enough to link law enforcement systems. Public safety information and communication systems must be interlinked with those of other state and local government systems (those that support emergency management, transportation, public health, social service and public utility related activities). State and local departments work daily with each other, but often this work is hindered by "stove piped" information systems. Improving each state's information technology

infrastructure will dramatically improve the ability of federal, state and local governments to identify emerging homeland security related or other public safety and public health threats.

These efforts should include establishing aggressive oversight of law enforcement and homeland security related activities. While the vast majority of law enforcement officers are honorable men and women doing a job that most people would be unwilling and unable to do, there are and will be those unethical individuals who will abuse the authorities entrusted to them. As we expand the universe of information available to law enforcement, we also expand the potential for abuse. I am hopeful that Congress, the courts and the media will continue to fulfill their vital oversight responsibility to uphold and protect the privacy rights and civil liberties of all Americans.

In conclusion, factual data analysis will strengthen national security, but only when critical law enforcement systems have been inter-linked – a preliminary step that to this date has not been.

Thank you for the opportunity to participate in this hearing.

Mr. PUTNAM. Thank you, Mr. Cohen.

At this point, I will recognize Mr. Turner if he has an opening statement and would like to give it now.

Mr. TURNER. Thank you, Mr. Chairman. I appreciate your having this hearing on this important issue.

As we listened to each of the testimonies, we certainly understand the importance of making certain we are protecting civil rights and making certain we do not have political views as a basis for discrimination in these processes or other types of discrimination we would want to avoid.

You can't help but listen to the importance of the task that is ahead of us to know that we must have a process of learning how to discern what an increased terrorist threat might be. In Mr. Steinhardt's testimony, he used the words, how would we be able to determine a terrorist from the 100 million Americans who fly. I think we are all aware that in the September 11 incident we weren't dealing with Americans, we were dealing with people on our soil who were carrying out an attack upon our country.

This discussion is important because we must find the balance there has to be in this process and a way we can use information to discern real threats without resulting to discrimination.

Thank you.

Mr. PUTNAM. We thank the gentleman and recognize the vice chairwoman of the subcommittee, Mrs. Miller, for questions.

Mrs. MILLER. Thank you, Mr. Chairman. I have a little cold going on today with my voice, so we will see how it holds up.

If I might followup with Mr. Cohen, I was particularly interested in your testimony about the sniper and some of the problems the locals had with information sharing. Is there anything you could tell us specifically to assist us in what you might think Congress could do, what our role is? I know so many of our States have very strong home rule and why that is particularly important, zoning issues and those kinds of things.

I think when it comes to national security or information sharing amongst law enforcement agencies, again the Federal Government has to be careful we don't get on the slippery slope there but you had that kind of experience with the locals. Is there anything you see Congress should be doing quickly here to expedite some of this information sharing that could have precluded some of the examples you used with the sniper which were quite vivid?

Mr. COHEN. I think actually Congress not only plays a critical role but quite frankly from what I am seeing, it is not going to happen unless Congress plays a role. One thing Congress can do immediately is take a look at what homeland security funding that is being disseminated out to State and local governments can be used for. You hear a lot of focus on response, which is important obviously, but as you look at the requirements of what funding can be used for, you very often do not see anything that indicates they could use it for information sharing.

State and locals have acknowledged this has been a problem prior to September 11. In the 1990's, there was a program within the Justice Department called the Integrated Justice Program which provided support to State governments to work with localities to integrate or link these information systems. The idea was

that as each State linked their intrastate criminal justice related information systems, you would then be able to link the 50 States into the Federal system.

During the sniper incident, one of the examples I didn't use is that a latent fingerprint was lifted from a robbery homicide in Montgomery, AL. That print was taken by the local police department, sent to the State of Alabama where it was run through their fingerprint system. There were no matches within the State of Alabama fingerprint system. Alabama was one of the States that was not linked to the Federal fingerprint system.

After a call by one of the snipers where they talked about a robbery homicide in Montgomery, AL, investigators from the Sniper Task Force traveled to Montgomery, AL, took the latent fingerprint on a piece of paper, traveled to Washington, DC, ran it through the Federal fingerprint system and identified the suspect Malvo. From there, they were able to identify the other suspect and then they were able to identify the car they were driving in a very short timeframe.

If Alabama had been linked to the Federal system, they probably would have identified that print prior to the sniper situation and when that car was stopped 4 hours before the first shooting in Wheaton, there would have been a Federal warrant in the system, and you may have prevented the entire event from occurring.

This is not massive data mining capability. This is basic system infrastructure that needs to be put into place. It is important, and this goes to Mr. Turner's point, how do you decide what information is important? Part of the problem is we adopt in this country a philosophy where somehow terrorism is somehow separate from crime and that is ridiculous because terrorists don't sit in their hotel rooms or their apartments thinking up their little plans and then come out only to carry out the plan. They commit drug trafficking offenses, illegal weapons trafficking offenses, document fraud, money laundering; they work with criminal organizations. They are intertwined with the criminal community throughout the world.

The best way and in fact most of the domestic cases that have been worked in this country since September 11 have all started off as criminal investigations by either a local police officer or a Federal agent. If we can link these criminal justice systems more effectively, it is not a technology issue but a willingness issue and we can look at terrorism and terrorist groups for what they are which is people driven by ideology to commit violent crimes, we can take a giant leap forward in making the country safer. For that to occur, funding has to be able to be used by State and local governments for these information systems, Congress has to insist that be a part of the philosophy that is adopted as our national homeland security planning.

Mrs. MILLER. That is absolutely true. You say a willingness. In my former life, as the chairman knows, I was the Michigan Secretary of State. We did all the DMV kinds of things in our State. As a consequence of that, we were responsible for feeding the LEAN machine, an acronym the police officers used for all the driving records and those kinds of things.

We had so many times when officers were abusing the system because they would get into it, find out their girlfriend's address, there were all kinds of things, even the reporters and the media were using it for things they shouldn't have used it for. So there are always those feeding those kinds of information systems and you certainly have to be vigilant about who is accessing it and penalties have to be given to those that abuse it as well.

You also mentioned the homeland security. This is something I think all of us see in our respective districts and States as the Federal Government is sort of feeding out this pot of money for homeland security. Unfortunately so often I see at the local level they are using it because the States are having a budget crunch, so they have had to lay off some police and fire and are using the homeland security to bring those layoffs back up to snuff, which I suppose is an important thing.

I think many of us, in our minds, were thinking about homeland security moneys for communications systems and border crossings and a lot of other kinds of things. That is something I think Congress does need to pay attention to, how it is actually being used on the home front.

I did have a question for Mr. Rosenzweig. You mentioned in your testimony, I have forgotten now, did you say Great Britain or Canada that has a system somewhat different from the American system where they have a point person, so they have someone who is accountable for their information sharing.

Do you have any specific recommendations? You mentioned here in our Nation, Congress has the responsibility for ensuring privacy and having these kinds of hearings. Do you think an appeals process outside the Congress as you mentioned, would be a good thing?

Mr. ROSENZWEIG. I think some form of review is absolutely essential. There is no doubt that however we construct these information technology systems to conduct advance factual data analysis, there will be errors. There will be what are known as false positives.

Especially in the CAPPSII Program, which impinges directly upon one of our cherished fundamental freedoms, the right to travel, no American citizen should be denied the right to travel within or outside the United States without a chance to have some redress and an ability to make a prompt argument that the determination is an error.

If it were technologically feasible and I don't know whether this will be because we don't know how the system will play out, I would like the appeals system to be at the airport, so that you can catch the next flight. That may prove to be impossible and it may well prove to be unnecessary if the parameters of CAPPSII are drawn tightly enough.

If you design the system such that the external identification queries merely create a name and verify that identity and that identity is checked against a terrorist list created through the use of intelligence sources and means and methods overseas that I don't know about and probably never will because I don't have a secret clearance, anybody who is red carded under that system and not permitted to fly is almost surely also going to be someone who

the authorities will immediately take into custody because of suspicion that they are in fact an active terrorist within the system.

That is how I conceive the development of the system and it is how I think TSA conceives it. Whether or not they can achieve that remains an open question. If they do achieve that, then the appeal from no fly will be in a different forum altogether, the court system where the suspected terrorist will soon be transported.

There should still be a system for an appeal of a yellow card determination where you are allowed to fly but are subjected to heightened scrutiny. However, the need for that to be an immediate process right at the airport is substantially diminished because yellow card means you fly unless the yellow card turns up something in which case you do not fly because you have the bomb in your luggage.

So there could be a more measured process by which one were given that appeal. Whatever the structure and architecture of the system, it is imperative that no American be denied the right to fly without the right to appeal.

I will add one other thing mentioned in my testimony. No American should be denied the right to fly, red carded, based solely on commercial data, data that is gleaned from publicly available commercial data bases because those data bases are maintained for different purposes, they have errors in them and they aren't intended to be terrorist identifiers.

If anybody is denied the right of travel, this Congress ought to tell TSA it ought to be based upon some positive indication from an affirmative, intelligence source that gives us a positive reason for thinking that this particular person, with this particular name ought to be on the list.

Mrs. MILLER. That really is the whole impetus of these programs, that TSA is able to do some sort of profiling to weed out the kinds of problems we might have at our airports.

I would like to ask one generally for the panel.

Mr. PUTNAM. We may need to get back to that. You have had a 10 minute round. We are going to move to Mr. Clay. I hate to cut you off because it is a good debate, but I will recognize the gentleman from Missouri for 10 minutes.

Mr. CLAY. I thank the witnesses for being here today. Thank you for your testimony.

I would like to begin by asking each of you to answer this question. Each of you has emphasized that Congress has an important policy role in balancing national security and privacy, however, the development of CAPPSII and the development of DARPA's Total Information Awareness have been difficult for Congress to review.

One of the reasons the Wyden amendment was passed was because Congress did not have sufficient information to allow the project to proceed. Now, we find the information Congress had then is no longer operative.

Similarly, Admiral Loy told us about all of his Federal Register notices and conferences but Congress still doesn't know what data is going to be used in CAPPSII or what rights citizens will have.

How can we assure that Congress has the information necessary and that all of the relevant committees consider that information before these programs go much further? Mr. Cohen.

Mr. COHEN. Congressman, as you were asking your question, I couldn't help but looking over your shoulder and seeing the portrait of Jack Brooks. I used to work for Chairman Brooks when he chaired the House Judiciary Committee. I was the deputy chief investigator for the committee. Chairman Brooks worked very closely with the ranking member of the committee on a number of issues.

Mr. CLAY. When I first met Jack Brooks 25 years ago, I worked here as a doorkeeper over there in the House. He ran the committee with an iron fist too.

Mr. Cohen. Yes, he did. I think back to the struggles we went through trying to conduct oversight. In my opinion as a law enforcement person, we are in a very uncomfortable time in this country because on the one hand, you have fear pervasive through society where people are saying things such as, maybe I am willing to give some of my civil liberties if just the Government will keep me safer. You have good people in law enforcement and government trying to come up with a solution that is a very complex and very scary situation where people are attacking this country.

At the same time, we are going through a period where folks are saying, if I am going to do my job effectively, I can't have that pesky Congress looking over my shoulder or media shouldn't be given accurate information, or the courts have no business telling us what to do. We are a nation at war.

It is a difficult balance because on the one hand, we have to protect sources and methods but on the other hand, there is a long history of abuses of authority, and there is a long history of law enforcement people even though I think most police officers and law enforcement folks in this country are people doing a job most would be unwilling or unable to do and they are honorable but there are bad people.

Today's LA Times runs a story about an LAPD officer who was using his access to law enforcement information systems to sell that information for his own personal gain. He ruined the life of hundreds of people. Abuses will happen. No matter how good intentioned an agency is in creating a system, there is always potential for abuse.

I think during these times, Congress has to be extraordinarily aggressive and the message has to get out that oversight isn't a bad thing, it is going to make our system stronger, it is going to help protect us better. What you find after you start taking a look at how terrorist organizations operate, you find a lot of the important information isn't secret information anyway. It is information that comes from community members, from basic law enforcement systems and non-law enforcement related government systems—drivers licenses, FAA, all those types of systems.

I think Congress by aggressively injecting a bit of reality into this process can play a real significant role.

Mr. CLAY. That pretty much serves as a way to fine tune our system of protections.

Mr. COHEN. Absolutely, Congressman. We worked very closely with the Justice Department, though it was a different party administration, on all types of issues. We worked closely with NSA and the intelligence community on a whole series of issues. Con-

gress is a very important player in this and cannot be excluded if we are going to be effective.

Mr. CLAY. Mr. Steinhardt, how can Congress assure that we have the necessary information?

Mr. STEINHARDT. I have a great deal of sympathy for your question. We have had a constantly shifting explanation of what the Total Information Awareness Program and CAPPSII Program are. Those charts come from DARPA and we blew them up to make that very point, that the explanation of these systems constantly shifts but that the initial explanation, whether the chart from DARPA or the Privacy Act notice filed by the TSA, are massive systems of surveillance.

It seems to me Congress has the right and the Constitutional duty to ask some hard questions of the administration about what exactly these programs will do, what data will be collected, who will they be trained on. It is clear they will be trained on American citizens. Whether or not there should be, as Mr. Turner suggested, and I tend to agree with him on this point, a separate set of rules that apply to non-Americans. It is clear both TIA and CAPPSII will apply to hundreds of millions of American citizens, American residents.

I would suggest in summary what you need to do is really employ a two step analysis. The first is you need to ask some hard questions about whether these systems will work. There are a lot of good people out there who are security experts, computer scientists, technologists who will tell you these systems are not likely to work. If they are not likely to work, then they become a diversion of our resources and creation of potential threat only to the point that you are satisfied they are likely to make us safer, not talking about 100 percent certainty. I understand nothing is 100 percent certain, but general certainty that the systems are going to make us safer, only if you are satisfied on that score do you then begin to ask the second set of questions which revolve around what is the cost to our freedoms and how can we cabin the systems so they don't cost us our freedoms.

You need to begin by asking that first question. Is it going to work, is it going to make us safer or is it going to create the illusion of security.

Mr. CLAY. You say there may need to be a bifurcated system or a two-tiered system where we treat American citizens one way and treat immigrants another way. You bring up a valid point. We may need to get a handle on who is here in this country and maybe scrutinize them in a different way than we do American citizens.

Mr. STEINHARDT. What I was trying to do, Congressman, was answer Mr. Turner's question about who would CAPPSII apply to. In my opening statement, I give the statistic that it applies to about 100 million Americans. I estimated the error rate 100,000 people if the error rate was 99.5. Mr. Turner asked a legitimate question, what about those people who are not American citizens. I was just emphasizing that both CAPPSII and as originally proposed the TIA systems were designed to go after American citizens. There is no question a different set of Constitutional standards applies to non-Americans. We can and should at some point talk about those but we need to recognize that these are not systems solely designed to

be applied to foreign visitors to this country. They are going to apply to hundreds of millions of American citizens.

Mr. CLAY. Thank you.

Mr. Rosenzweig.

Mr. ROSENZWEIG. The answer to the question how is a very simple one. You have more power than you think you have or you know you actually have more power, the power of the purse, the power of public observation and ultimately powers of subpoena.

I was on a program talking about the Patriot Act, an NPR program with Congressman Conyers about 6 months ago. As you may imagine, we don't necessarily agree on a number of things but this was at the time when the Department of Justice was refusing to provide data on its use of subpoena powers to the Judiciary Committee. One of the things that we agreed on wholeheartedly was the necessity for the Department of Justice or any other executive branch to provide you with information.

I don't see in these charts a nefarious mutation of policy. I see the natural product of the development of an idea that starts as an outside the box conception in an agency that we designed for the purpose of doing outside the box thinking, that ultimately gets refined as it is subjected to public scrutiny such that it is indeed likely a variation on the original idea that is more sensitive to public liberty concerns.

That is not DARPA's mission. DARPA's mission is to have the wild hairbrained ideas. It is the other people in the executive branch's idea to say, whoa, make sure you do it the right way and it is your mission to say to the executive branch, really make sure you do it the right way.

I actually see the trend between those two charts that Mr. Steinhardt seems to think of as a demonstration of the bad motivation that initially went into this as actually an example of the system working. Congress did the right thing with part of the Wyden amendment by saying, tell us what you are doing and sometime today you are going to get 500 pages, 300 pages, I don't know what they will give you, on what TIA is doing.

I am sure Mr. Steinhardt is going to study that carefully, I am going to study that carefully, you and your staff are going to study that carefully, and we can build from there. So do more of what you are doing is the answer.

Mr. CLAY. Thank you for that answer.

Mr. PUTNAM. I thank the gentleman.

Mr. Steinhardt, you made several references in your written and verbal testimony to the surveillance society. Has the ACLU's definition of an acceptable level of surveillance in society changed since September 11?

Mr. STEINHARDT. We have never been opposed to strong security measures. My colleague, Rich Nochime for example, testified before what was then known as the Gore Commission in the prior administration, on aviation security about the need to do several things. One was to fully secure the cockpit doors in airplanes; second was to x-ray all the package or otherwise test all the baggage going into the cargo hold; third was to put armed guards on the planes. We have never been opposed to security.

The questions we have been raising are does the security that is proposed work? Many of these proposals simply will not work. They will not make us safer. Second, how can we retain our liberties in the face of the ever advancing march of technology which makes it easier to collect data about us, to correlate that data, to mine that data? I can show you my device that does e-mail and phone and keeps my calendar but we need to begin to put some rules around this technology.

I had the opportunity the other day to visit with Dr. Popp, the deputy director of the Total Information Awareness Program. He was showing us some slides about TIA. He was showing a slide that showed the role of different agencies in the TIA Program. In the bottom righthand corner of that slide, and I cannot forget this, was a balloon that said "policy" and the remarkable thing about that balloon was it was empty. There is no policy other than the Wyden amendment. There is no policy that really constrains what can be done with TIA. That is Congress' role, you need to begin to develop those policies. You can't leave them to the governmental officials who build these systems.

Mr. PUTNAM. Everyone else in society has sort of lost their footing since September 11 and are trying to regain it as to what is acceptable. Prior to September 11, red light cameras and face recognition technology at a Super Bowl may not have been acceptable. After September 11, it may be. There is this effort on the part of society and it is reflected in the Congress of trying to regain our footing as to what is an acceptable level of surveillance in our lives.

My question was whether or not the same process had been undergone in ACLU but let me move on.

There has been a growth, perhaps an explosion, in the number of local and State law enforcement agencies who have begun their own intelligence divisions, agencies, operations that are probably subject to less scrutiny than the Federal agencies have been up to. Would you comment on your awareness of municipal or State efforts in this regard and your concerns or observations on their progress, beginning with Mr. Cohen?

Mr. COHEN. You are right, for a number of reasons State and local law enforcement have expanded their exports in two things, one in the collection, analysis and dissemination of information and intelligence, especially on the State level as an intelligence dissemination hub. The State of California has created a Counterterrorism Information Center. The State of Maryland is establishing a similar capability where crime and terrorism related information will all come into a central analytical facility and be disseminated out to Federal, State and local entities. The State of Arizona is building a similar capability.

At the same time, many local agencies are focusing on this whole issue of intelligence and creating their own intelligence divisions.

The reason the States are having to step up and do this is because there is a perceived lack of capability coming from the Feds in this area. Whether it is because the Federal Government doesn't have the infrastructure or the capability itself or whether it is a different perspective on what information sharing is, a number of State and local governments have felt they are in a better position to conduct this analysis and dissemination.

From the standpoint of creating local intelligence groups, local law enforcement for the most part sees the correlation between crime and terrorism, and while they tend to be under less Federal scrutiny unless they are using Federal funds for technology systems that facilitate movement of this information, they tend to be under pretty extensive local scrutiny because of past problems.

The city of Denver, for example. The city council and the local courts are very heavily focusing on the efforts of the Denver City Police Department to collect intelligence information. When we work with police departments, we say as long as you continue to remember things like due process, probable cause and you are linking your information collection activities to criminal activity, you are in good shape. If you start straying from that area and start looking at collecting information that may not be related to criminal behavior, you need to be very careful.

Mr. STEINHARDT. Let me followup what Mr. Cohen just said because the Denver case is actually an ACLU case. We are not opposed to the Federal Government and local and State law enforcement agencies talking to one another as some might suggest. We are concerned about what happened in Denver where you had the Denver police collecting information about lawful protesters who were exercising their first amendment rights and creating what amounted to spy files about those individuals.

It is both a diversion of the resources of the Denver Police Department from far more critical things they could be doing and a deprivation of rights. Denver is not alone. That occurred before September 11 but Denver is not alone as a representative of that problem. In New York, the incumbent administration had a policy for a period of time that they simply would not approve any parade permits, so people who wanted to exercise their first amendment right to protest were prohibited from doing it.

The consequence was they denied a permit to what turned out to be 500,000 or 600,000 people who wanted to hold a demonstration in front of the U.N. before the Iraqi war broke out. The classic exercise of their first amendment rights to petition their government for a redress of their grievances as the first amendment says, the consequence was from a security perspective that you had hundreds of thousands of people wandering through streets of Manhattan in a disorganized way that made us less secure rather than more secure.

We need to recognize that even in these times, we are not suspending the Constitution, we are not suspending the Bill of Rights, we need to apply those resources in a way that makes the most sense, that is efficient and effective.

Mr. ROSENZWEIG. I think the answer to your question depends upon the subject matter of the intelligence gathering. To a very real degree the tools and methods by which we are going to identify terrorists reside principally at the Federal level, the CIA, NSA, DOD, FBI, Homeland Security.

The creation of intelligence divisions in the States is to be welcomed. Any enhancement of our abilities to identify terrorists is great but I guess from my perspective, unless those intelligence capabilities are linked with the Federal system and thus far they are not so linked, they result in a duplication of effort to some degree.

That is the nature of our Federal system. Indeed it was created in some ways to cause inefficiency, the division between Federal and State and locals is designed to cause governmental inefficiency.

In the case of terrorists questions, that may be an inefficiency we can no longer afford.

Mr. PUTNAM. Do you believe Mr. Rosenzweig, that government should be restricted to publicly available data sources?

Mr. ROSENZWEIG. With appropriate safeguards, no.

Mr. PUTNAM. My time has expired. I will recognize the gentleman from Ohio, Mr. Turner.

Excuse me, Mr. Lynch?

Mr. LYNCH. No.

Mr. PUTNAM. Mr. Turner.

Mr. TURNER. Mr. Steinhardt, in listening to your testimony and reading over the written statement you have given us, I agree with your concerns and the problems you have identified in these types of systems. The issues of we can't catch everyone, there will be failures of the system. Timothy McVeigh would not be someone who would have been identified. Abuse of government, the fact that other uses of this information might be found. Civil liberties, the fact that innocence would be identified, that there could be creep, that we needed due process for those aggrieved, that criminals may subvert the system, that once the system is constructed, those who really want to get beyond it can and the issues of cost benefit analysis.

Your conclusion of then don't do this leaves me with the question of what is the alternative. We know what we are doing now doesn't work and we have all seen 85 year old grandmothers with their grandchildren traveling who have gone through increased security measures and we all agree pose no risk to us.

I would love to hear from you what is the alternative besides just increased security. We all know, even in the highest crime areas of urban America, you could put a policeman on every corner and still not have an impact on crime necessarily. What alternatives in intelligence gathering or in looking at intelligence would you find acceptable or would you suggest be pursued?

Mr. STEINHARDT. I think that is an important question. To my mind the first alternative is physical security. That remains our best alternative. We have taken some steps in air travel that are working pretty well. We put air marshals on the planes, we strengthened cockpit doors, we x-ray baggage. There are some additional things we ought to be doing. We are still not doing luggage matching to determine whether someone checking luggage on the plane actually got on the plane. There are a number of things we could be doing in addition to what we are doing that is physical security.

We are not opposed to the notion that the government have a properly constituted watch list of persons who we believe are engaged in terrorist activities which are criminal activities, that be circulated and people be carefully checked against it but that is not what CAPPSII is.

CAPPSII is designing a much larger system of investigation of 100 million Americans plus 10 or 15 million non-U.S. persons who arrive here every year. When we say we think CAPPSII is the

wrong alternative to the problem, it is not to suggest we think either there are not additional physical security measures we can take, nor is to suggest we think the Government should be prohibited from compiling a generally accurate list of persons who are not permitted to fly. If you have identified one of those persons, you trigger the normal criminal process. If you identify someone who is a terrorist, then the likelihood is you have sufficient cause to arrest them and bring them to trial.

Mr. TURNER. How would that list be made, the watch list you are talking about, how would that be composed, how would you achieve that list?

Mr. STEINHARDT. We certainly would have to go beyond what we now have. About a year ago some of us met with some persons who were then in the Department of Transportation, I suppose they are in Homeland Security now, who described the current watchlist as 1,000 guys named Mohammed and I am not exaggerating that.

If we have sufficient information about individuals to believe that they intend to cause us harm, that they have engaged in criminal activities, terrorist activities which are also criminal activities, then it seems to me it is appropriate to circulate a list to security officials and check to see if they are trying to fly.

Mr. TURNER. The second question is for Mr. Steinhardt again. You indicated the Constitutional standards for non-Americans would be different and there is some level of acceptable tracking that could be done. Would you be willing to submit to this committee additional information as to what you would consider to be an acceptable tracking system for non-American citizens?

Mr. STEINHARDT. Absolutely. We will provide the committee with additional information. I will ask my colleagues who work on those issues to help me. We will submit some information.

Mr. TURNER. The next question I have goes to all the panel members, starting with Mr. Rosenzweig.

I participated in a panel at the American War College at Maxwell Air Force Base. One of the questions asked by someone attending was can America right a religious war? One of the biggest issues we all came down to which I thought was pretty startling was how do you define a religious war. If your enemy declares a religious war, you are in one whether or not you believe you are in a religious war yourself.

We define ourselves being an immigrant population as everyone, every religion, every ethnicity. Governmentally we consider ourselves to be nonreligious. Yet the rest of the world does not necessarily organize that way. There are areas of the world that tend to be more homogeneous, that are not immigrant populations. So when we have an area of the world that identifies America as an enemy or a target, we are going to find ourselves in a situation where by trying to discern who our enemy is, we are in fact crossing that line into an area where America feels very uncomfortable because of our inherent definition of ourselves of being made up of everyone.

In looking at that issue, what are your thoughts on the Constitutional issues that we face, the political issues we face, our concerns being an immigrant population of making certain as we preserve our definition of a nondiscriminatory society, we still have the abil-

ity to discern where there is a conflict that is coming from an isolated area of the country that may be more homogeneous and may have a different view of why it is at war with us?

Mr. ROSENZWEIG. That is a very difficult question to answer. Let me offer two thoughts.

The first thought is that in some very real ways, the promise of advanced technologies that we have been discussing is to minimize the need for the use of characterizations and categorizations that Americans inherently find difficult, racial profiling, religious profiling, that sort of thing.

When we talk about CAPPSII or TIA as an intrusion into privacy, we have to understand that it really is not a one-way rachet. It is really a rebalancing the privacy because there are more intrusions in electronic data that is out there about you that will probably result in substantial reductions in the amount of physical intrusions that occur to American people as they go through the airports, the body searches and things.

Another consequence of a successful CAPPSII Program, if we can develop one and if it can work, I don't know whether it will work and history is littered with people who will say airplanes won't fly and automobiles will never work. Assuming it works, if we can get a system that is better at pinpointing who it is that is an appropriate target for enhanced scrutiny because of indicators out there, that decreases our need and may even eliminate the need for us to rely upon the fact that a person is a practitioner of Islam who was born in Yemen and has moved to the United States, characterizations we don't want to use.

The second answer, second aspect of it is we are going to have to accept that as a cost in the end. It is not a cost anyone willingly accepts and we shouldn't use those sorts of characterizations for any except the most extreme and significant threats. I would say don't use it for drugs, don't use it to catch wife beaters, there is a whole host of valuable things we do but all of them pale in significance compared to the security of Americans and their safety.

If we can find no other way to do it, then we are going to have to with a lot of oversight so we try and do it the best way we can with the least amount of intrusion. Those are the only answers. That is not a good answer, not a satisfying answer but we are in a very unsatisfying situation that is not the product of our own beginning.

Mr. STEINHARDT. As you said, I agree we need to have better coordination among law enforcement agencies whether it is State or Federal, local or Federal but the question remains what is it these systems will evolve into? I was thinking as I prepared for this testimony about the experience with the Social Security number. My parents when they first received their Social Security numbers back in the 1930's were promised the Social Security number would not be used to do anything other than to administer this brand new pension program.

My children on the other hand, if you fast forward a few decades, were given their Social Security numbers at birth and it is quite clear it has become not only a unique identifying number in our society but it has very real consequence for millions of Americans

who have become the victim of identity thieves who use that Social Security number as the linchpin for their theft.

I fear that in the Internet age in which we live where everything is sped up, period between when my parents got their Social Security number and my children got theirs is going to be tremendously compressed. That if we build systems like TIA and CAPPS II, in the end they are going to be used for not purposes that are unauthorized, although they will that is not what I am worried about, I am worried about what will become the eventual authorized purposes for systems that allow that sort of intrusion into our lives, that allow that sort of ability to correlate what would seem to be these disparate and unrelated facts about us.

Mr. COHEN. I think your two questions are linked because if we do this right, we shouldn't have to fight religious wars. Terrorists aren't dangerous because they have dangerous thoughts or they say dangerous things. They are dangerous because their political or religious ideology motivates them to do violent acts against people, places and things. The danger comes from the violent act. They don't commit those violent acts in a vacuum. They deal with criminal organizations, other political organizations. They move about the world.

There are ways to target them and prevent them from doing what they intend to do without it becoming a religious war. We do it the same way we target violent international weapons trafficking organizations and violent international drug trafficking organizations who use many of the same terrorist-like tactics to promote their goals. So they commit violent acts, sometimes mass murders motivated by greed.

In my opinion, a mass murder committed or motivated by political ideology is no more sinister than a mass murder committed because of mental illness or because of the intent to promote a criminal goal.

I think this goes to your question, what do we do if we are not going to invest in the CAPPS II system or TIA? I think it becomes a question of priorities. We have limited funding; that is the reality of life. Is it more important to build the TIA system or the CAPPS II system or is it more important to conduct a comprehensive national threat assessment where the Federal Government works with State and local governments to identify potential targets? Is it more important to create a system so that once that threat assessment is done, we can constantly reevaluate and reprioritize it based on information that comes from the Federal level?

Is it more important or a higher priority to map out the business processes of how international terrorist organizations work with domestic groups like black militant organizations, white supremacist organizations, latin american drug traffickers?

I have to tell you I fundamentally disagree with my panelist's position that one of the most important components in identifying terrorists operating in this country, the information is going to come from the intelligence community. Investigation in North Carolina into cigarette smuggling by local sheriffs resulted in the discovery of a terrorist cell where they were using the proceeds from cigarette sales to fund Hezbollah operations. It didn't start off as an investigation that came from intelligence sources but because some

local deputy sheriffs were told by community people there were some suspicious behavior going on.

DEA agents, FBI agents began an investigation in San Diego into an heroin trafficking organization. Come to find out, that organization is involved in shipping surface to air missiles to Latin American terrorist groups.

An organization coming in from Canada bringing precursor chemicals for the production of methamphetamine resulted in dismantling an incredibly large methamphetamine production. Guess what we found out afterwards? They were funneling the proceeds of the sales of those precursor chemicals to Middle Eastern terrorist organizations.

The vast majority of the cases on terrorist organizations that have taken place since September 11 weren't initiated by information that came from the intelligence community. They were initiated because a local police officer, a Federal agent, a community member reported something suspicious, and a criminal investigation began. They found out later when they linked information that came from the intelligence community that these folks had a tie with terrorist organizations.

I am not saying the intelligence community doesn't have a role. That would be ridiculous to say that. It is only when we recognize, if we are going to be truly serious about preventing terrorism in this country, this philosophy that terrorism is worked on this path and crime investigations are worked on a separate path and we have to make it difficult that we don't share that information; until we recognize that is a nonproductive way to do it, we are not going to be able to put in place a system in this country that allows Federal, State, local law enforcement to best protect the people who live here.

Mr. TURNER. Thank you.

Mr. PUTNAM. You have made the point Mr. Cohen rather eloquently about the nexus between drugs and weapons trafficking and the source of financing for terrorist organizations. Mr. Steinhardt and Mr. Rosenzweig have both testified either in written submissions or verbally that at bare minimum, if we are to deploy TIA and CAPPS they should not be expanded beyond national security issues into criminal activity.

If we criticize an inability to connect the dots because the criminal agencies, the law enforcement agencies aren't talking to the intelligence community or the Department of Defense, why would we restrict the ability of TSA and others using best technology practices to pick up a sniper, a weapons trafficker, a drug trafficker, a murder, a kidnapper? How would we justify to the parents of a kidnapped child that we had technology that could have picked up that person at the airport but we only use that for terrorists? At what point would you draw that line where national security threats cross the threshold into criminal activity? I would direct that to Mr. Steinhardt and Mr. Rosenzweig?

Mr. ROSENZWEIG. I think the principal difference between Mr. Steinhardt and I is that he doesn't believe you are going to be able to maintain that line, that in the end the reality of politics will cause Congress and the administration, whether Democrat or Republican, to follow that downward path.

The reason and one of the only reasons I am willing to take the step of looking at TIA is because I believe you can make that line and I believe you should.

Mr. PUTNAM. Where do you put the line?

Mr. ROSENZWEIG. I think the line is where we are talking now, national security, the maintenance of the security of all the citizens of the United States against broad threats of terror that are likely to result or may result in the deaths of tens of thousands, thousands of us, is a class category distinction in my mind.

To be honest with you, if I didn't think you could draw and maintain that line, I would be joining with Mr. Steinhardt because the power of this technology to be a potential for abuse and for intrusion is not insignificant. To my mind, the risk is worth it if it is going to be used in this narrow range of circumstances that are the most significant. You can't define the line but I think it is easy to say that September 11 is a lot different than chasing down deadbeat dads. Deadbeat dads who don't pay their alimony and child support are bad people.

Mr. PUTNAM. You have laid down those two markers, let us move inward from deadbeat dads to Pablo Escobar or move further to a major weapons trafficker, or further to someone who is a financier of Al-Qaeda but is not a known operative.

Mr. ROSENZWEIG. The lines are difficult no doubt and there will be room for argument in the gray area where it is. I would say the financier falls on the side of the line where I would use it. I would say Pablo Escobar, however grave a threat he is to Americans, is not a fundamental threat to American security and does not have as his fundamental purpose the intent to kill tens and tens of thousands of Americans.

The difficulty in drawing the line is often used as the slippery slope argument against even beginning the discussion. I stand with Justice White who wrote in response to the slippery slope argument, we are rationale human beings, we can draw lines, we can debate where we want to draw them, but to say we cannot draw them is to despair of our rationality. I am paraphrasing obviously. That way lies despair. That way, don't do this at all. in which case, we are tossing away potentially our greatest technological advantages if these things work and condemning quite possibly Americans to death or admitting we can't draw a line and we are going to travel down the road to a police state or surveillance state where TIA and CAPPS II and other systems like that are used to dun me for my unpaid traffic tickets.

I hope we can stop somewhere along that slope.

Mr. PUTNAM. Mr. Steinhardt.

Mr. STEINHARDT. The ACLU has never opposed the intelligence agencies and the criminal law enforcement agencies talking to one another when there is evidence of a crime. We had plenty of evidence before September 11 those terrorists who hijacked those planes were going to commit a crime. There was nothing in law then, certainly nothing now in law that prevents those agencies from talking to one another. That ought to be the touchstone here which is whether or not you have evidence of criminality. If that is the case, the information can be shared and should be shared.

I would think if the TIA had evidence at the airport that Pablo Escobar or some other wanted criminal was presenting himself, the right response is call the cops, bring them in and have them make the arrest.

That is very different from the question of how do you design these systems. Do you design them to be an adjunct to law enforcement or do you design them for the purpose for which they originally were to be created which is as security systems.

To the extent we are going to have these systems, I would suggest we design them as security systems. I am sure if Admiral Loy were here he would say that is his first priority. He is in the security business, not the law enforcement business. I know of nothing in law that would prevent the TSA if they came across a wanted felon from calling the criminal law enforcement agencies to make the arrest.

Mr. PUTNAM. You have made points back and forth, one following Mr. Forman's comments we are not going to fund anything until it is proven effective and the other your philosophical opinions on the privacy issues. Is your primary objective the deployment of TIA, which has not occurred, or the development and deployment of CAPPS II which has yet to occur? Is your objection based on the ineffectiveness argument that it is not going to work or the intrusiveness argument which is that it is going to work too well and bring in innocent people?

Mr. STEINHARDT. I fear it will be both. Systems like that are not going to work in the sense that they are not going to make us more secure. I don't mean 100 percent security, no one believes we can achieve 100 percent security but a reasonable degree of extra security.

Second, if we build systems like that, they are inevitably going to be used for other purposes, even as they don't protect us, they will be used for other purposes. In fact, as they don't protect, the impulse is going to be to make them more intrusive, to gather more information, to use them in different ways. That will be the response, their lack of efficiency, their lack of effectiveness. That is what I fear about systems like TIA and CAPPS II. Build it and they will come with all sorts of other uses for systems like that and they inevitably will be used for other purposes just as my parents' Social Security numbers are used for a host of other purposes now.

Mr. PUTNAM. You specifically cite in your testimony your objection to Admiral Loy's comment. In fairness to Admiral Loy, his comment was in response to my question and he couched his response by saying he would not expand the use of CAPPS II beyond air travel without specific congressional authorization if I remember correctly.

You object to using the same technology for air travel on passenger cruise lines and rail travel. If we deploy a technology to presumably increase the security of air travel, why would we deliberately choose not to deploy that same technology to rail and cruise ships? Do we presume they won't select those transportation modes as a target?

Mr. STEINHARDT. We object to the technology whether employed in air travel or rail or shipping. Your response I sense is what I assume will happen which is if we build one of these systems, say

CAPPS II, you make an excellent point, if we build the system, why not apply it in other areas and we would employ it for a whole host of other reasons, some of which are completely unrelated to the security of our transportation. That is exactly what I think will happen if we build CAPPS II or TIA. We will use them in other ways.

There is no good answer in a sense to your question which is why not use it in x or y case.

Mr. PUTNAM. If you are right and it doesn't work, we shouldn't put it anywhere?

Mr. STEINHARDT. That is right.

Mr. PUTNAM. But if it does work, I think it would be silly to use it in air travel but leave all rail passengers vulnerable. I would lead the charge in Congress in response to your objection. Your objection is well founded and people like me would say if it works for air, it ought to work for rail and passenger cruise lines because clearly the people who wish us ill have a range of targets to choose from.

My time has expired. I will recognize the gentleman from Massachusetts if he has questions.

Mr. LYNCH. Let us go back to the airline model. Right now we have just a purely random system, so my mom, 82 years old, coming down for the First Lady's luncheon last week gets screened and it is completely random. We need to move from that model. Clearly we are wasting a lot of resources on people who aren't legitimate threats. That is not effective.

Is there a system out there with some criteria that would be acceptable in terms of honing down the number of suspects that would receive more robust screening at airports? I know it is terribly problematic but when you have a situation like we have where there is a group that has declared war against this country and we are at pains under our Constitution to make sure we don't simply respond to that by stigmatizing and labeling all members of that group as suspects, we still have an overriding primary responsibility to protect the citizens of our country. There is the dilemma.

Is there anything you gentlemen can agree on that might provide a more effective screening process?

Mr. ROSENZWEIG. That is what TSA is searching for. As of now, the alternate to the random screening is a various set of heuristics they use but they are so widely known to the public that it is easy to avoid. For example, if you buy a ticket late, less than a half hour or hour before you board, you are going to get additional screening. The answer to that for the terrorist is easy, buy your tickets 14 days in advance.

To the extent systems are currently in place that attempt to supplement random screening, they are essentially compromised and of little or no value. To the extent that we are creating the CAPPS I No Fly list, it isn't really working and just about anybody who does a little research can figure out how it is created. It is fundamentally compromised.

You need a different heuristic. If the CAPPS II system or something like it isn't developed and adopted, then you are going to be left only with random searches or I guess the last option is the very narrowest definition, the hard name list. We cull every intelligence

source and we get 27,000 people we think are terrorists and we use that name list. If we don't add name verification and identity checking to it, which is the part of CAPPS II that people like Mr. Steinhardt find objectionable for understandable reasons, the name list is useless because the obvious answer is change your name. It is not a very hard thing to do and it is not a very hard thing to assume somebody else's identity.

The only way we can get beyond the current system I think is something like the model they have developed in CAPPS II. If we make the decision we don't want to do that for other extrinsic policy reasons, that is OK but then we are going to be doing heightened physical security, heightened random screening, more privacy intrusions of the direct and immediate personal sort that your mother experienced, and it is a tradeoff. We will take that type of privacy intrusion as opposed to the privacy intrusion of the name and identity verification of CAPPS II.

For me, I would make the other choice but you can't really say there is no rationality to the objection.

Mr. LYNCH. Are we missing one other option? Isn't there the possibility that we could have people self prove, low susceptibility or low likelihood that they might be a terrorist, people who fly frequently, if they came forward voluntarily and said, I fly so often I can't be dealing with the selection process all the time. I will come in and basically lay all my cards on the table and this is who I am and I will agree to go through some type of enhanced identification process. Maybe it is biometrics or something like that.

Mr. ROSENZWEIG. The trusted traveler program has at least three problems. It is another possible answer. One, the depth of inquiry necessary to make somebody a trusted traveler if it is low enough to make it an efficient process is probably going to miss people. If it is high enough that it will actually be effective in screening out terrorists who try to get into the program, it will take longer than the FBI screening that now delays senatorial confirmation by 6 months.

You are talking about lots more people, so it is going to be hard and it is subject to the same discovery of the methodology problems that any other screening system is, which is that the terrorists, once they learn there is a new system, can game it. You can't predict for certain, but for sure terrorists will try and suborn that system that setting themselves up as trusted travelers.

No system is going to be perfect. That is at least a reasonable alternative that allows people to volunteer to make the choice of which type of privacy intrusion they will accept, the physical one at the airport or the electronic one in getting the trusted traveler, so at least it has a virtue of choice. That is a reasonable alternative to think about.

Mr. LYNCH. Thank you, Mr. Chairman.

Mr. PUTNAM. The ACLU has stated TSA will "drown security screeners in an ocean of private information. Some of the data will be fraudulent and much of it just plain wrong." That statement was printed after our last hearing and is in direct conflict to what Admiral Loy described as CAPPS II doing. What is that assertion based on?

Mr. STEINHARDT. It is based on the privacy notice which the Department of Transportation published which they now admit was their first description of the CAPPS II Program. I have had the opportunity to meet with Admiral Loy. We spent 3 days with his staff at Wye River and had a long discussion about the CAPPS Program. I have great faith in Admiral Loy and I believe he is a man of good will. I believe his staff are people of good will.

The initial description of the CAPPS II Program was the one they published in the Federal Register. There has been a shifting description of what CAPPS II now is. They describe it differently in Wye River than they did to representatives of the European Commission we met with a couple of weeks ago. It is difficult to know exactly what CAPPS II is. It is difficult to know what is in the black boxes they are going to check after they do the identity checks. It is important to remember CAPPS II as they currently describe it is a two-step process. The first is an identity check, name, home address, home phone number and date of birth. The second is a check against the black boxes and we don't know what is in the black boxes. They have described what is in the black boxes differently at different times. It seems to me it certainly is Congress' responsibility to try to find out what is in the black boxes.

Mr. PUTNAM. Does the use of factual data analysis or data mining automatically suggest an erosion of civil liberties?

Mr. STEINHARDT. I guess the short answer to that question is no. The question is are we going to build systems of the size and complexity of either TIA or CAPPS II which inevitably will be used to erode civil liberties and will inevitably be used for purposes other than the purposes for which they are now being proffered.

Clearly we engage in a certain amount of data mining, police officers, law enforcement officers engage in a certain amount of data mining anytime they do an investigation. So we are not inalterably opposed to the concept that law enforcement or intelligence agencies engage in factual investigations. There is a form of data mining going on every time they do that.

Mr. PUTNAM. But I presume your preference and your agreement with its proper role is after an incident and after an investigation has begun rather than prior to a bad occurrence, an event? In other words, you are investigating, your data mining, you are narrowing down based on suspects that were developed as a result of evidence that was collected after a bad thing happened as opposed to prospectively looking for patterns among innocent people because a bad thing has not yet occurred. Is that a fair characterization of your position?

Mr. STEINHARDT. I suppose it is but importantly we hold that view because we don't think what you have just described actually works. Does it in fact make us safer? That is not to say they had some good reasons to suspect a person is going to commit a crime, they can't investigate but to search through what amounts to billions of pieces of data looking for patterns in the sort of speculative way that TIA would do it, I don't think they have demonstrated you can pick out the bad guys and it won't wind up being a diversion of scarce resources that could be more wisely spent on other enterprises.

Mr. PUTNAM. Again, your objection is based on its ineffectiveness, not its intrusiveness?

Mr. STEINHARDT. No. What I suggested is there is a two step process here. First, the obligation it seems to me is on the part of the proponents of the systems to demonstrate it will be effective; that you as a Member of Congress ought to vote to appropriate them funds to do x instead of y because x is going to be effective. That is the first question. We don't even have to reach the civil liberties issues if they can't demonstrate it is going to be effective.

If a proposal is effective or reasonably effective, I don't mean 100 percent efficiency, then we need to begin to ask the question how do we balance our freedoms against whatever intrusion that proposal will cause. The first question is, is it going to work.

Mr. PUTNAM. That is a fair point.

There are volumes of information already publicly available about any given individual. Technology now allows us to access—in seconds rather than days—when political campaigns or newspaper reporters dispatch investigators to the tax collector's office, the property appraiser's office, the supervisor of elections office, and the county court house to look for criminal records and things like that. It can all be theoretically accessed in seconds if the stovepipe data bases are connected.

Assuming factual data analysis can be an effective law enforcement and national security tool, at what point on the list of transactional data on the chart you provided, which of those categories of data then become inappropriate? Is financial data appropriate or inappropriate? Is educational data appropriate or inappropriate? What about travel history, medical history, entry into the country? What then becomes appropriate and what is not? Is it only things that are already publicly held information that is accessible to any American and not just the TSA law enforcement investigator or is it every conceivable thing law enforcement can get their hands on to prevent another September 11?

Mr. STEINHARDT. You know the difficulty we have now as you suggest is the fact so much information has become available. TIA crystallized that not only are these disparate pieces of information available out there publicly both to the government and to non-governmental actors, but now they can all be tied together. That is what TIA proposes to do. Paint this portrait of us.

There is a lot of information on that chart I don't think the government ought to have access to unless it has some reasonable cause to have access. That is what the fourth amendment requires, medical information, financial information, education records, all those sorts of things.

It is important to look at the overall construct. TSA proposes to build a system that ties together all these individual strands about our lives to create this portrait of us. That is what I meant by the surveillance society. TIA is an example of how this surveillance society would operate. Tie all the strands together, paint these portraits, the portraits may or may not be true to life but they will be painted and we will have to live with the consequences of having those portraits painted. That is the direction in which we are moving.

It seems to me the Congress can step in and say wait, we need to develop some rules about how we are going to use not only individual data but when and how you can tie together all this data. Congress did the right thing with TIA when it called time out and said you can't use it on Americans and you can make a report to us on how the system works, whether it works and what its consequences are for civil liberties.

Mr. PUTNAM. Mr. Rosenzweig.

Mr. ROSENZWEIG. I think Mr. Steinhardt and I have a different conception of how TIA is going to operate which is one of the reasons why congressional oversight is vital. As I understand it, in terms of pattern analysis, in terms of assessing patterns within the data streams, this isn't going to be a sifting in of millions of pieces of information of education and medical records and all. It is going to be pushing out into the data a query based upon models developed by people who have sat around and said if we are going to blow up the Golden Gate Bridge, what are the things we are going to have to do that would leave trails in data space, what purchases are we going to have to make, what travel are we going to have to do.

It is clear as far as that inquiry goes, the success or failure of TIA will turn upon the utility of our model. If we develop the model of people who rent trucks and buy fertilizer, that will capture not only Timothy McVeigh but most farmers in Nebraska. That would be a really bad model.

It will need to be a broader model, maybe rent trucks, buy fertilizers, pay cash, have previous membership in the Montana Militia, etc. until it gets to a narrow enough group. Otherwise, it is useless.

For access to the highly personalized information of a particular person, the likelihood of that being a necessity will only increase when the number of names gets down to very small, particularized groups. That is as it should be. To be candid, if we have a list of five names that some intelligence source in Lebanon has given us are in the United States and are planning terror, it is appropriate I think to want to be able to link the data bases together so we can try and find out whether or not we can get the information on these people.

To a large degree, TIA is about increasing efficiency. All the information on that list, your financials, your medical, education, is already available to the government once your name becomes a legitimate subject of inquiry. Almost none of those areas of data information have privacy restrictions that prevent access to them in the case of criminal investigations. In almost all of those instances, the data can be accessed without notice to the original source of the data, the individual who is the subject of the investigation. Often notice is required to the data holder, your bank, your medical provider, that sort of thing.

TIA is not going to change those rules or shouldn't change those rules. The same rules that apply today to the rights of law enforcement to have access to private information about you should apply in the future when you access through TIA.

TIA will instead of taking as it took the FBI 9 months and 100 agents to develop a picture of what the 19 terrorists did in the 2-

months before September 11, it will allow it to happen more quickly. If we have a narrowly enough focused search, that is a good thing, not a bad thing.

Mr. PUTNAM. The gentleman from Ohio, do you have further questions?

Mr. LYNCH. No.

Mr. PUTNAM. The gentleman from Massachusetts?

Mr. TURNER. No.

Mr. COHEN. May I?

Mr. PUTNAM. Please do.

Mr. COHEN. I think some of the last comments were actually apropos and right on. I think the key to building this type of system is to have the ability to take in real time intelligence information and make modifications. For example, when Mohammed Atta and his roommate received within a 6-week period a number of suspicious wire transfers that all fit within the requirements of suspicious transaction reports, it should have been put on file with the Treasury Department. That in itself does not mean they are part of a hijacking scheme. It could be they are a drug trafficker, or they could be importing legitimate goods.

If the system is structured right, it would also be able to pull in additional information such as intelligence information which indicates people are going to flight schools. The same individual was on an FAA report leaving a plane on a runway in Miami International Airport. The key is to make sure the system is flexible enough and structured enough so that it can bring in these different types of data sources.

To your earlier question about where do you draw the line, you can't draw the line. There is no line because they are all interlinked. I would argue if you build a system that is only going to help identify foreign terrorists but not identify someone like Tim McVeigh whose goal was very similar, or you are going to somehow try to separate artificially identifying folks involved in violent crimes from people involved in violent terrorist acts, you are not going to be able to construct a system and you are going to pour a lot of money into something that is not going to work very effectively.

The flip side of that, if you go into the design of the system understanding that not only can it help you protect the Nation from terrorism but it is also going to help you protect the streets of our communities from violent criminal activity and build the system based on that understanding, you can then put in the protections which would reduce abuses of that capability.

Mr. PUTNAM. You don't think there is an ability to draw some line on acceptable criminal behavior that would be enforced, a line at which you would not pick up people who are behind in paying their child support but you would pick up someone who just escaped from a south Florida prison?

Mr. COHEN. I think the way you structured your question earlier sort of identifies or illustrates the difficulty. The person who is involved in failure to pay child support; the person who is involved in cigarette smuggling; the person involved in making fraudulent drivers licenses; may actually be a terrorist. If you create a system

that artificially separates those different actions, you may be building a system that isn't as effective as it could be.

If you go back and look at the activities of the hijackers in the time period preceding the hijackings, you find they had all kinds of run-ins with local police and local authorities. It wasn't until we went back after the fact that we were able to see if we only had a system that would have allowed us to connect all these dots together.

The other thing I would say is we don't want to necessarily build a system that only helps address the last attack. We have to build a system that is going to allow us to prevent the next attack, whether a suicide bombing, some other type of attack different than hijacking an airplane and crashing it into a building.

Mr. PUTNAM. You make the point in your testimony when you describe the breakdowns in law enforcement information sharing that the sniper attacks could have been prevented. You point out the State of Alabama's data base doesn't have access to Federal data bases, correct?

Mr. COHEN. Yes, sir.

Mr. PUTNAM. Later in response to a question, you said the creation and buildup of these local and State counterintelligence, counterterrorism, domestic information gathering operations is a good thing because you are spreading the eyes and ears around the country and you are developing people who have unique local expertise and things like that. I am paraphrasing you but you essentially said it was a good thing that the city of New York now has a tremendous intelligence operation as well as others.

Are we spending the money in the right places if we are building up brand new counterintelligence networks in city police departments and State law enforcement agencies when they don't even have access to the data bases on common criminals?

Mr. COHEN. No, we are not and that is part of the problem. We have to recognize while prevention and response activities ultimately include at a great level local authorities, local authorities themselves cannot do it alone. It is a very bad use of money to simply allow each individual local jurisdiction to come up with their own homeland security strategy that is not connected with their neighbor, not connected on a regional basis and not coordinated on a statewide basis and feeds in. What you described is exactly what is happening right now.

We haven't come up with a detailed, national comprehensive plan that defines the roles and responsibilities of how the city of Miami links with Dade County from how they are going to work together, what assets they are going to merge and how that fits into the whole statewide approach.

The problem is because there hasn't been, from a State and local perspective, that strong direction and because at the State and local level, people feel they need to be doing something, you are beginning to see the emergence of a lot of non-linked, duplicative efforts.

Mr. PUTNAM. So we are creating more stovepipes even as we seek a streamlined data base?

Mr. COHEN. Absolutely. My concern is that 2 or 3 years down the road when we are doing the after action study on how we spent

this money, people will find we spent billions and billions and have not gone as far as we could have and in some respects, the funding has been wasted.

Mr. PUTNAM. You were pretty blunt in your testimony that very little progress if any has been made in information sharing and analysis across the law enforcement community since September 11, even though everyone acknowledges the problem. What is the single greatest obstacle to that coordination or what is causing this breakdown or this failure?

Mr. COHEN. It is not a lack of money; it is not technology. It is leadership and whether on a State or national level, we haven't made it a priority yet to fix this problem. If you think about the whole universe of what is homeland security, that is a pretty big challenge to have to deal with. There are a lot of issues and a lot of people identifying what the priorities should be. Should it be ports, air travel systems, CAPPS, TIA? I think we need to take a step back, need to stop operating in the emergency response mode of thought and start looking long term.

We do not have the resources in this country at the State and local level or even the Federal level to continue our approach to homeland security which I call the "security guard" approach. We don't know what the real targets are, so we are going to guard everything or harden as many things as we can. We are going to pull police officers out of their communities and do what we can to protect every nuclear power plant, every water treatment plant, every bridge. It is just impossible.

The only way to counter that is to sort of reboot the computer and rethink the way we are doing it. We need to integrate homeland security into the day to day business of government, need to make sure everybody understands this is something we have to deal with every day, and we have to structure our information and communications systems in such a way that we are able to pull key data out of those to identify emerging trends.

Is a broken lock at a water treatment plant a maintenance issue, or is it a terrorist organization or a criminal organization probing the security of that facility? We don't have the ability to do that today. A lot of Governors, a lot of mayors are beginning to think this is the way of the future. We have to make sure the Federal funding supports that thought process.

Mr. PUTNAM. Then their ticket to more Federal money is to create the greatest threat scenario possible for their community?

Mr. COHEN. You bring up an interesting point. There is no way for anyone to counteract. Obviously in the real world, local governments need money, so they will say we will use homeland security as a way for us to get additional funding to address infrastructure issues. I don't think that is necessarily a bad thing except for the fact there is no mechanism today for someone to say, city of Houston, your threat is actually higher than Salt Lake City, therefore, you should be prioritized.

We have formulas that were created in years prior to September 11. We have formulas based on demographics or population because we haven't done a comprehensive, nationwide threat assessment and because we don't have a system in place that allows us to constantly reevaluate that on an ongoing basis. We have no way

to really determine whether one city is more at risk than another except for conjecture, mathematical models, and non-specific or non-confirmed intelligence information.

I come from a background of information driven policing. Police departments around the country have begun to become very effective in pulling data from a variety of sources, whether abandoned buildings, abandoned vehicles. They understand what are the causal factors of crime. They identify the data element they need, and management holds people accountable for addressing crime issues and preventing crime.

That is the same approach we should be taking in homeland security but we have not identified that baseline yet to begin the process. From a priority perspective, that should be our top priority—comprehensive nationwide threat assessment. Create the baseline, and create a system so that we can constantly update and reevaluate. That is what guides funding decisions and operational decisions also.

Mr. PUTNAM. Is there a difference in your outlook or your fears between a Federal agency engaging in factual data analysis inhouse and them doing it on a contracting basis with a private firm? Is it irrelevant? Does it matter one way or the other to you as far as the applicability of privacy laws and things like that? Mr. Steinhardt.

Mr. STEINHARDT. Increasingly what we are finding is that it is difficult to draw a distinction between when the Government is doing something and when the private sector is doing something because government both contracts with the private sector, provide services and information and sometimes it compels the private sector to provide it with services or information. So it is very difficult.

It seems to me though that when the Government is involved, it makes sense to apply Constitutional principles to the action whether the Government has hired someone to do it for it or not and that ought to be the touchstone that the most efficient way to use our resources at this point is to apply the Constitution. It makes Constitutional sense and makes law enforcement efficiency sense. We should be applying scarce resources we have in those circumstances where we have reasonable cause to believe someone has or will commit a crime. That ought to be the touchstone rather than these massive sets of speculations that TIA or CAPPS II suggest.

One place to begin spending our scarce resources is to fix what is broken. I was stunned a few weeks ago to read a notice in the Federal Register by the Department of Justice in which they said the National Crime Computer [NCIC], was a data base they could no longer stand behind the accuracy of. They wanted to be exempted from the requirement that this data base, our central repository of criminal justice records, is accurate.

Mr. PUTNAM. Who did that?

Mr. STEINHARDT. The Justice Department. That was a stunning development. For many years, many of us believed the NCIC was full of garbage but here the Justice Department is saying not only do we agree it is full of mistake but we are no longer willing to stand behind it. That is frightening both from a civil liberties perspective because of the mistakes that are going to be made but it is also frightening from a security perspective, that you have a cen-

tral data base that law enforcement is relying on at both the State, local and Federal levels and it is simply full of inaccuracy. That is the kind of thing that might be an appropriate opportunity for this subcommittee to look at, what systems do we already have in place, how accurate are they?

The ACLU is not opposed to the concept we have a centralized repository of criminal justice information but it ought to be accurate both from a civil liberties and a security perspective.

Mr. PUTNAM. Mr. Rosenzweig.

Mr. ROSENZWEIG. To answer your question, the key to oversight and therefore control is accountability. To the extent that outsourcing the operation of a system diminishes the accountability of Federal officials who you will call to account for the operation of the system, it is to be generally disfavored.

There is obviously no hard and fast rule and there are some things that are far more efficient to use contractors for and we should obviously want to do whatever we do with the government dollar in the most efficient and effective manner.

As a general rule, I would urge you to ensure that any system that is put in place retains a high degree of accountability in high level administration officials who you can demand come here and tell you how CAPPS II or TIA is working or not working.

Mr. PUTNAM. The Wyden amendment was put on the Omnibus Bill so it is a 1-year issue. What do each of you see as being Congress' timeline for action and what do you see that action as being between now and the expiration of the Wyden amendment? What does the post-Wyden world look like from your perspective and the timeline for that?

Mr. ROSENZWEIG. I would like to see Congress consider a program like TIA and authorize additional research in the program. I would urge the research contain a series of guidelines as to what Congress considers an acceptable program, one that retains accountability. We didn't talk about the necessity of an audit trail but I have listed a dozen different recommendations in the written testimony that in suitable legislative language ought to be incorporated in any authorization.

When and if the concept proves itself to be potentially effective, since I agree with Mr. Steinhardt that we don't have to address the liberties questions unless and until the research says we can do the thing, those who would use it, the FBI, DHS, CIA, come back and seek further authorization to deploy the system.

Mr. STEINHARDT. Actually your first responsibility begins today. Today is literally the deadline for DARPA and other Federal agencies involved to submit a report to the Congress in response to the Wyden amendment on the TIA Program.

We suggested in my testimony a series of questions we hope you will ask about that report. It seems to me the Congress needs to carefully scrutinize this report before it authorizes any further construction of the Total Information Awareness Program, you certainly ought to put a halt to it until you satisfy yourselves that it both will be effective and will protect our freedoms.

Mr. PUTNAM. Recognizing that DARPA is a research agency and their business is high risk research, isn't it a bit unusual to apply a proof of success test to a research agency whose very mission is

to continue to work things through until they prove they are successful or not. We don't make cancer research funds contingent upon finding the cure by a certain date. We understand the nature of the scientific process is you continue to seek answers based on a hypothesis and the data you collect in your experimentation. Is that a bit of an unusual standard?

Mr. STEINHARDT. Here you are talking about fundamental liberties at stake, in some respects the construction of our society. I don't think it is unusual at all for Congress to say before we appropriate half a billion dollars, to build a prototype system, TIA, that we want some demonstration that this is likely to work as opposed to other possibilities we have for that half a billion dollars that could be spent.

The Wyden amendment does not prohibit them from going forward with research and they are going forward with research. I am curious to see what this report says about what they regard as the likely effects from this program and how they came to those conclusions. I urge you to look closely at that as well. As an appropriator you need to make decisions about how to spend half a billion dollars. You need to have some assurances that there is a likelihood of success.

Mr. PUTNAM. Mr. Cohen.

Mr. COHEN. The only thing I would add to what Mr. Rosenzweig and Mr. Steinhardt said is at the end of the day is that the best use of half a billion dollars? If our local and State criminal justice systems, which are going to be a key part of an effective TIA system, still don't work; if in Maryland you are only able to enter one warrant per person, so if Montgomery County has an open container warrant for John Cohen, and the Eastern Shore wants to put a robbery warrant in the system, you can't do it because of the way the system is structured, the question becomes: where would half a billion dollars be spent more effectively, research on TIA or making sure each State has a robust and interconnected, integrated justice system?

Mr. PUTNAM. Before we conclude, is there other final comments any of you would like to make or a question of a fellow panelist that you have not heard today?

Mr. STEINHARDT. I was going to suggest I think the one thing we all agree on is that we have taken enough of the committee's time.

Mr. PUTNAM. This is a very important issue and this is not the end of the committee's work on this issue. As all of you have pointed out, the report due today will be an important next step to the further congressional involvement in this matter.

I want to thank all of you for your outstanding insight and comments and I thank the members of the subcommittee who participated.

In the event there may be additional questions we did not get to today, the record will remain open for 2 weeks for submitted questions and answers which all of you will be expected to respond to.

Thank you all very much.

[Whereupon, at 12:15, the subcommittee was adjourned, to reconvene at the call of the Chair.]

○